# *VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH) TERHADAP *WEBSITE*

**Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan**

SKRIPSI

Oleh :

Muhammad Yaqi

11180910000125

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH JAKARTA**

**2023 M / 1444 H**

# *VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH) TERHADAP *WEBSITE*

**Studi Kasus : Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan**

*Diajukan untuk memenuhi persyaratan memperoleh gelar sarjana komputer (S.Kom)*

Oleh :

Muhammad Yaqi

11180910000125

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH JAKARTA**

**2023 M / 1444 H**

# LEMBAR PERSETUJUAN

## *VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH) TERHADAP *WEBSITE*

**Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan**

Skripsi

Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom)

Oleh

Muhammad Yaqi

11180910000125

Menyetujui

| Dosen Pembimbing 1 | Dosen Pembimbing 2 |
|---|---|
| | |
| **Arini, S.T., M.T.** | **Siti Ummi Masruroh, M.Sc** |
| NIP. 197601312009012001 | NIP. 198208232011012013 |

Mengetahui,

Ketua Program Studi Teknik Informatika

**Dewi Khairani, M.Sc.**

NIP. 198205222011012009

# LEMBAR PENGESAHAN UJIAN

Skripsi berjudul "*Vulnerability Assessment* dan *Penetration Testing* (VAPT) Menggunakan Metode *Zero Entry Hacking* (ZEH) Terhadap *Website* Studi Kasus Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan)" yang telah ditulis oleh Muhammad Yaqi dengan NIM 11180910000125 telah diuji dan dinyatakan lulus dalam sidang Munaqasyah Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta pada tanggal 26 Juni 2023. Skripsi ini telah diterima sebagai salah satu syarat memperoleh gelar sarjana Strata Satu (S1) Program Studi Teknik Informatika.

Menyetujui,

| Penguji I | Penguji II |
|---|---|
| Hendra Bayu Sutrisno, M.Kom | Tabah Rosyadi, M.A |
| NIP. 198212112009121003 | NIP. 196207141989031004 |

Menyetujui,

| Pembimbing I | Pembimbing II |
|---|---|
| Arini, S.T., M.T. | Siti Ummi Masruroh, M.Sc. |
| NIP. 197601312009012001 | NIP. 198208232011012013 |

Mengetahui,

| Dekan Fakultas Sains dan Teknologi | Ketua Prodi Teknik Informatika |
|---|---|
| Husni Teja Sukmana, S.T., M.Sc, Ph.D. | Dewi Khairani, M.Sc. |
| NIP. 197710302001121003 | NIP. 198205222011012009 |

# PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa:

1. Skripsi ini merupakan benar hasil karya asli saya yang diajukan untuk memenuhi salah satu persyaratan memperoleh gelar Strata 1 di UIN Syarif Hidayatullah Jakarta.
2. Semua sumber yang saya gunakan dalam penulisan ini telah saya cantumkan sesuai dengan ketentuan yang berlaku di UIN Syarif Hidayatullah Jakarta.
3. Apabila kemudian hari terbukti karya ini bukan hasil saya sendiri atau merupakan hasil jiplakan karya orang lain, maka saya bersedia menerima sanksi yang berlaku di UIN Syarif Hidayatullah Jakarta.

Tangerang Selatan, 12 Juni 2023

Muhammad Yaqi

11180910000125

# PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI

Sebagai civitas akademik UIN Syarif Hidayatullah Jakarta, saya yang bertanda tangan di bawah ini :

| | |
|---|---|
| Nama | : Muhammad Yaqi |
| NIM | : 11180910000125 |
| Program Studi | : Teknik Informatika |
| Fakultas | : Sains dan Teknologi |
| Jenis Karya | : Skripsi |

Demi perkembangan ilmu pengetahuan, menyetujui untuk memberikan UIN Syarif Hidayatullah Jakarta Hak Bebas Royalti Non-eksklusif (*Non-Exclusive Royalti Fee Right*) atas karya ilmiah yang berjudul :

**_Vulnerability Assessment_ dan _Penetration Testing_ (VAPT) Menggunakan Metode _Zero Entry Hacking_ (ZEH) Terhadap _Website_ Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan**

Dengan Hak Bebas Royalti Noneksklusif yang diberikan ini, UIN Syarif Hidayatullah Jakarta berhakmenyimpan, mengalih formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak ciptaatas karya tulis ini. Demikian pernyataan ini saya buat dengan sebenar-benarnya dan tanpa paksaan dari pihak manapun.

Jakarta, Juni 2023
Yang Menyatakan

(Muhammad Yaqi)

# KATA PENGANTAR

## *Assalamualaikum Wr. Wb*

Dengan memanjatkan puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "*Vulnerability Assessment* dan *Penetration Testing* (VAPT) Menggunakan Metode *Zero Entry Hacking* (ZEH) Terhadap *Website* Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan", sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Jurusan Teknik Informatika.

Selama penyusunan skripsi ini tentunya terdapat banyak kesulitan dan hambatan yang dialami oleh penulis, baik dalam pengumpulan data, implementasi metode dan lain sebagainya, namun berkat bantuan dari berbagai pihak, kesulitan tersebut dapat diatasi. Hal ini merupakan suatu kebahagian bagi penulis dapat mempersembahkan kepada kedua orang tua, keluarga besar, dan pihak-pihak yang telah ikut andil dalam penyelesaian skripsi ini.

Sebagai bentuk penghargaan izinkan peneliti untuk menuangkannya dalam bentuk ucapan terima kasih sebesar-besarnya kepada:

1. Bapak Husni Teja Sukmana, S.T., M.Sc., Ph.D. selaku Dekan Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.
2. Ibu Dewi Khairani, M.Sc. selaku ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta.
3. Ibu Arini, S.T., M.T. sebagai Dosen Pembimbing I dan Ibu Siti Ummi Masruroh, M.Sc. Sebagai Dosen Pembimbing II yang telah membimbing, memotivasi, dan terus mendorong peneliti untuk menyelesaikan skripsi ini. Peneliti mengucapkan banyak terima kasih untuk waktu, tenaga, dan dukungan serta kritik dan arahan yang membangun agar skripsi ini dapat diselesaikan dengan baik dan dengan hasil yang sesuai.
4. Dosen-Dosen Program Studi Teknik Informatika yang telah memberikan ilmunya selama penelti menuntut ilmu di UIN Jakarta.
5. Kedua Orang tua, Kakak, dan Adik saya yang selalu menyayangi, mendidik, dan memberikan motivasi, nasihat, doa dan dukungan serta bantuan baik secara moril maupun materil sehingga peneliti dapat melalui masa-masa sulit saat menuntut ilmu di bangku perkuliahan.
6. Mamaci, dan Ericca yang selalu memberi semangat dengan cara yang berbeda dari kebanyakan orang dan merupakan sesuatu yang saya butuhkan.

7. Almer, Bari, Mira, Parhan dan Keluarga besar RUMCI yang telah membangun semangat, dan keinginan saya untuk turut serta menyelesaikan skripsi ini.
8. Sahabat saya Ido yang selalu memberikan doa dan motivasi bagi diri saya untuk terus maju.
9. Teman-teman di Puslitpen (Rizka, Aufa, Barra, Naufal, Syifa, Kak Adel, Kak Hanum) yang selalu memberi bantuan saat ada kesulitan.
10. Teman-teman di kelas E Teknik Informatika 2018 yang telah memberikan dukungan, semangat, bantuan, doa, ilmu dan pengalamannya untuk peneliti dapat menyelesaikan skripsi.
11. Seluruh pihak yang telah banyak berjasa terhadap proses penyelesaian skripsi ini yang tidak dapat penulis sebutkan satu persatu namun hal ini tidak mengurangi sedikitpun rasa terima kasi peneliti.
12. Diri saya sendiri karena sudah mampu bertahan melewati berbagai hambatan dan tetap semangat menyelesaikan skripsi ini.

***Wassalamualaikum Wr. Wb***

Jakarta, Juni 2023

Muhammad Yaqi
NIM:11180910000125

Penulis : Muhammad Yaqi

Program Studi : Teknik Informatika

Judul : *VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH) TERHADAP *WEBSITE* Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

# ABSTRACT

In the current digital era, the need for information is increasing along with technological advancements. However, with the increased use of information and communication technology, threats that can endanger system security also emerge. Statistical reports indicate an increase in the number of traffic anomalies and cybercrime cases in Indonesia, with a total of 44,776,891 traffic anomalies, and the highest number of anomalies occurring on August 3, 2022, reaching 3,103,770. Therefore, enhancing system security is crucial as an effort to protect systems and networks from unwanted attacks. One of the agencies that utilizes websites as an essential service is the Investment and Integrated One-Stop Service Agency of South Tangerang City. Although there have been no reports of hacking on the agency's servers, preventive measures and security measures have been implemented. However, to ensure system security, Vulnerability Assessment and Penetration Testing need to be conducted. The author performed Vulnerability Assessment and Penetration Testing using the Zero Entry Hacking method. The tools used for vulnerability scanning in this research include Uniscan, OWASP ZAP, and Acunetix. The results of this research successfully identified vulnerabilities with 3 medium-level and 4 low-level ratings. Vulnerability measurement after testing was conducted using the Common Vulnerability Scoring System (CVSS) v3.1 tool to help recommend priority fixes that need to be implemented.

**Keywords:** *Vulnerability Assessment, Penetration Testing, Zero Entry Hacking* (ZEH), *Common Vulnerability Scoring System (CVSS), Website.*

Penulis : Muhammad Yaqi

Program Studi : Teknik Informatika

Judul : *VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH) TERHADAP *WEBSITE* Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

# ABSTRAK

Dalam era digital saat ini, kebutuhan akan informasi semakin meningkat seiring dengan perkembangan teknologi. Namun, dengan peningkatan penggunaan teknologi informasi dan komunikasi juga datang ancaman yang dapat mengancam keamanan sistem. Laporan statistik menunjukkan adanya peningkatan jumlah anomali trafik dan kasus kejahatan siber di Indonesia sebesar 44.776.891 anomali trafik dengan jumlah anomali tertinggi terjadi pada tanggal 3 Agustus 2022 sebesar 3.103.770. Oleh karena itu, peningkatan keamanan sistem menjadi penting sebagai upaya untuk melindungi sistem dan jaringan dari serangan yang tidak diinginkan. Salah satu instansi yang memanfaatkan *website* sebagai layanan penting adalah Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan. Meskipun belum ada laporan peretasan pada server instansi tersebut, tindakan pencegahan dan pengamanan telah dilakukan. Namun, untuk memastikan keamanan sistem, *Vulnerability Assessment* dan *Penetration Testing* perlu dilakukan. Penulis melakukan *Vulnerability Assessment* dan *Penetration Testing* dengan metode *Zero Entry Hacking*. Adapun *tools* yang penulis gunakan untuk melakukan *vulnerability scanning* pada penelitian ini antara lain, *Uniscan, OWASP ZAP,* dan *Acunetix*. Hasil pada penelitian ini berhasil ditemukan kerentanan dengan 3 tingkat *medium* dan 4 tingkat *low*. Pengukuran kerentanan setelah dilakukan pengujian dilakukan dengan alat bantu *Common Vulnerability Scoring System (CVSS)* v3.1 untuk membantu merekomendasikan prioritas perbaikan yang perlu dilakukan.

**Kata Kunci:** *Vulnerability Assessment, Penetration Testing, Zero Entry Hacking* (ZEH), *Common Vulnerability Scoring System (CVSS), Website*.

## DAFTAR ISI

*LEMBAR PERSETUJUAN*.....*i*

*LEMBAR PENGESAHAN UJIAN*..... *ii*

*PERNYATAAN ORISINALITAS*..... *iii*

*PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI* .....*iv*

*KATA PENGANTAR*.....*v*

*ABSTRACT* .....*vii*

*ABSTRAK*.....*viii*

*DAFTAR ISI* .....*ix*

*DAFTAR GAMBAR*.....*xiv*

*DAFTAR TABEL*.....*xvii*

*DAFTAR LAMPIRAN*.....*xviii*

*BAB I PENDAHULUAN*.....*1*

**1.1 Latar Belakang** .....**1**

**1.2 Identifikasi Masalah**.....**8**

**1.3 Rumusan Masalah**.....**8**

**1.4 Batasan Masalah**.....**9**

**1.5 Tujuan Penelitian** .....**11**

**1.6 Manfaat Penelitian** .....**11**

1. Bagi Penulis.....12
2. Bagi Universitas .....12
3. Bagi Intansi Terkait.....12
4. Bagi Masyarakat.....13

**1.7 Metodologi Penelitian**.....**13**

1.7.1 Metode Pengumpulan Data....13
1.7.2 Metode Pengujian dan Analisis....13
1.7.3 Jenis Penelitian....13

**1.8 Sistematika Penulisan....14**

***BAB II LANDASAN TEORI....16***

**2.1 Konsep Dasar Sistem....16**
2.1.1 Pengertian Sistem....16
2.1.2 Karakteristik Sistem....17

**2.2 Konsep Dasar Informasi....19**
2.2.1 Pengertian Informasi....19
2.2.2 Nilai dan Kualitas Informasi....20

**2.3 Konsep Dasar Keamanan Sistem Informasi....22**
2.3.1 Konsep Dasar Keamanan....22
2.3.2 Keamanan Sistem Informasi....26
2.3.3 Tipe-tipe Ancaman Keamanan....31
2.3.4 Kerentanan Sistem....33
2.3.5 Serangan-serangan pada *Web Server*....37
2.3.6 Jenis-jenis *Web Server*....38
2.3.7 *Website*....41
2.3.8 *Web Security*....44
2.3.9 *Vulnerability Assessment* dan *Penetration Testing*....46

**2.4 *Common Vulnerability Scoring System* (CVSS)....50**
2.4.1 Pengertian *Common Vulnerability Scoring System (CVSS)*....52

**2.5 Jaringan Komputer....53**
2.5.1 Pengertian Jaringan Komputer....53
2.5.2 Klasifikasi Jaringan Komputer....54

**2.6 Protokol Jaringan....55**
2.6.1 Model Referensi OSI....55

2.6.2 Kerentanan Pada Masing-Masing *Layer* mengacu pada *Framework* TCP/IP *Protocol* .....58
2.6.3 *Transmission Control Protocol*/*Internet Protocol* (TCP/IP) .....59
2.6.4 *UDP (User Datagram Protocol)* .....60
2.6.5 Perbedaan TCP *(Transmission Control Protocol)* dan UDP *(User Datagram Protocol)* .....61
2.6.6 Topologi Jaringan .....62
2.6.7 *Ports* .....66

**2.7 Internet .....68**

**2.8 Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan .....68**

**2.9 *Hacker* .....71**
2.9.1 *Black Hat* .....71
2.9.2 *White Hat* .....71
2.9.3 *Grey Hat* .....71

**2.10 Pengujian Aplikasi .....72**
2.10.1 Teknik Pengujian *Software* .....72

**2.11 Pengujian dan Analisis .....73**
2.11.1 *Zero Entry Hacking* (ZEH) .....76
2.11.2 Tahapan *Zero Entry Hacking* (ZEH) .....77

**2.12 Penelitian Eksperimen .....78**

**2.13 *Tools*/Teknologi yang Digunakan Untuk *Penetration Testing* .....79**
2.13.1 *Who Is* .....79
2.13.2 *The Harvester* .....80
2.13.3 *What Web* .....81
2.13.4 *CXSecurity* .....82
2.13.5 *Google Hacking Database + Google Dorking* .....83
2.13.6 Terminal .....84
2.13.7 Nmap .....85
2.13.8 OWASP ZAP .....85

2.13.9 Uniscan .....86
2.13.10 Acunetix.....87
2.13.11 Weevely .....88
2.13.12 Burp Suite .....89

**2.14 Literatur Sejenis .....90**

***BAB III METODE PENELITIAN*.....*95***

**3.1 Metode Pengumpulan Data .....96**
3.1.1 Studi Lapangan .....96
3.1.2 Studi Pustaka .....97

**3.2 Metode Pengujian dan Analisis.....98**
3.2.1 Roadmap Penelitian .....98

**3.3 Kerangka Penelitian.....99**
3.3.1 *Reconnaisance* .....100
3.3.2 Pemindaian (*Scanning*).....101
3.3.3 Eksploitasi Celah Kerentanan (*Exploitation*) .....102
3.3.4 Pasca Eksploitasi (*Post Exploitaiton*).....102

***BAB IV ANALISIS DAN IMPLEMENTASI SISTEM .....103***

**4.1 Analisis Alat Kebutuhan Pengujian .....103**

**4.2 Implementasi Sistem .....104**
4.2.1 Tahap *Reconnaisance* (Pengintaian Target) .....104
4.2.2 Tahap *Scanning* (Pemindaian).....119
4.2.3 Tahap Eksploitasi (*Exploitation*) .....124
4.2.4 Tahap Post Exploitation.....131

***BAB V HASIL DAN PEMBAHASAN*.....*138***

**5.1 Hasil Identifikasi Kerentanan .....138**

**5.2 Hasil Eksploitasi .....139**
5.2.1 *Cross Site Scripting* (XSS) .....139
5.2.2 *Clickjacking* .....140

**5.3 Pengukuran Kerentanan Menggunakan *Common Vulnerability Scoring System* (CVSS).....140**

**5.4 Rekomendasi Perbaikan .....143**

***BAB VI KESIMPULAN DAN SARAN*.....*146***

**6.1 Kesimpulan .....146**

**6.2 Saran.....146**

***DAFTAR PUSTAKA*.....*148***

***LAMPIRAN*.....*148***

# DAFTAR GAMBAR

Gambar 2. 1 Serangan Secara Pasif .....23
Gambar 2. 2 Serangan Secara Aktif (Denial of Service) .....24
Gambar 2. 3 Segiti CIA.....27
Gambar 2. 4 Persyaratan Keamanan Komputer dan Jaringan.....28
Gambar 2. 5 Interupsi.....31
Gambar 2. 6 Modifikasi .....32
Gambar 2. 7 Intersepsi .....32
Gambar 2. 8 Fabrikasi.....32
Gambar 2. 9 Proses VAPT Jaringan .....46
Gambar 2. 10 Vulnerability Assessment dan Penetration Testing Life Cycle.....47
Gambar 2. 11 Security Assessment Category Level.....47
Gambar 2. 12 Kalkulator CVSS V3.1.....53
Gambar 2. 13 OSI Model.....56
Gambar 2. 14 Pembentukan dan Pemutusan Koneksi TCP .....60
Gambar 2. 15 Topologi Bus.....63
Gambar 2. 16 Topologi Ring .....63
Gambar 2. 17 Topologi Star.....64
Gambar 2. 18 Topologi Tree.....64
Gambar 2. 19 Topologi Mesh .....65
Gambar 2. 20 Topologi Wireless .....65
Gambar 2. 21 Topologi Jaringan Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan.....66
Gambar 2. 22 Well-Known Ports.....67
Gambar 2. 23 Information Gathering dengan Whatweb.....70
Gambar 2. 24 Information Gathering dengan Ping.....70
Gambar 2. 25 Tahapan Zero Entry Hacking (ZEH).....77
Gambar 2. 26 Cara Menggunakan Whois .....80
Gambar 2. 27 Cara Menggunakan theHarvester.....81
Gambar 2. 28 Cara Menggunakan WhatWeb .....82

Gambar 2. 29 Cara Mengakses CXSecurity .....83
Gambar 2. 30 Contoh Penggunaan Google Hacking Database.....84
Gambar 2. 31 Terminal .....84
Gambar 2. 32 Contoh Penggunaan Nmap.....85
Gambar 2. 33 OWASP ZAP .....86
Gambar 2. 34 Contoh Penggunaan Uniscan .....87
Gambar 2. 35 Contoh Penggunaan Acunetix.....88
Gambar 2. 36 Cara Menggunakan Weevely .....89
Gambar 2. 37 Cara Menggunakan Burp Suite .....90
Gambar 2. 38 Visualisasi Mapping Literatur Sejenis .....94
Gambar 3. 1 Rencana Penelitian .....100
Gambar 4. 1 Hasil Who Is-1 .....105
Gambar 4. 2 Hasil Who Is-2 .....106
Gambar 4. 3 Hasil Pencarian Dukungan Ipku.in.....107
Gambar 4. 4 Hasil Pencarian Dukungan Bgp.he.net.....107
Gambar 4. 5 Hasil WhatWeb .....108
Gambar 4. 6 Hasil The Harvester.....109
Gambar 4. 7 Hasil Pengintaian CXSecurity Nginx.....110
Gambar 4. 8 Daftar Dork PHP dalam GHDB .....110
Gambar 4. 9 Wp-login.php?action=register.....111
Gambar 4. 10 Php?sql=select.....111
Gambar 4. 11 Wp-config.php .....112
Gambar 4. 12 Phpunit.yml .....113
Gambar 4. 13 Download.php?file=.....113
Gambar 4. 14 Php Version.....114
Gambar 4. 15 Files containing juicy info.....114
Gambar 4. 16 Admin/php.....115
Gambar 4. 17 Phpmyadmin/setup .....115
Gambar 4. 18 Guest/auth_login.php .....116
Gambar 4. 19 Wp-config.php.bak.....116
Gambar 4. 20 PhpMiniAdmin.....117

Gambar 4. 21 Index of PhpMyAdmin .....117
Gambar 4. 22 phpInfo .....118
Gambar 4. 23 Xmlrpc.php.....118
Gambar 4. 24 Hasil Ping .....119
Gambar 4. 25 Hasil TCP Scan .....120
Gambar 4. 26 Hasil WhatWaf.....121
Gambar 4. 27 Hasil Scanning OWASP ZAP .....121
Gambar 4. 28 Hasil Uniscan .....123
Gambar 4. 29 Hasil Scanning dengan Acunetix .....124
Gambar 4. 30 Content Security Policy (CSP) Header Not Set .....125
Gambar 4. 31 Cross Site Scripting (XSS).....126
Gambar 4. 32 Burp Clickbandit .....127
Gambar 4. 33 Clickjacking Attacks .....128
Gambar 4. 34 Cookie No HttpOnly Flag & Cookie Without Secure Flag .....129
Gambar 4. 35 Informasi Javascript dari Domain Pihak Ketiga .....129
Gambar 4. 36 X-Content-Type-Options Header Missing.....130
Gambar 4. 37 Clickjacking Check Menggunakan Clickjacker.io.....130
Gambar 4. 38 X-Powered-By.....131

# DAFTAR TABEL

**Tabel 2. 1** Kelebihan dan Kekurangan Nginx .....39
**Tabel 2. 2** Kerentanan pada Web Server .....40
**Tabel 2. 3** Kerentanan pada Web berdasarkan OWASP TOP 10.....42
**Tabel 2. 4** Kelebihan dan Kekurangan Metode Penilaian Kerentanan.....50
**Tabel 2. 5** Perbedaan TCP dan UDP .....61
**Tabel 2. 6** Kelebihan dan Kekurangan Metode Penetration Testing.....73
**Tabel 2. 7 Literatur Sejenis**.....90
**Tabel 4. 1** Perangkat Keras (Hardware) Penelitian .....103
**Tabel 4. 2** Perangkat Lunak (Software) Penelitian.....103
**Tabel 4. 3** Tools yang digunakan untuk Penelitian .....104
**Tabel 4. 4** Hasil Port Scanning Nmap .....120
**Tabel 4. 5** Hasil Vulnerability Scanning dengan OWASP ZAP .....122
**Tabel 4. 6** Hasil Vulnerability Scanning dengan Acunetix .....124
**Tabel 4. 7** Tabel Pengukuran Kerentanan dengan CVSS.....131
**Tabel 4. 8** Summary Tahap Reconnaisance .....132
**Tabel 4. 9** Summary Tahap Scanning .....133
**Tabel 4. 10** Summary Tahap Exploitation.....134
**Tabel 4. 11** Summary Tahap Post-Exploitation .....135
**Tabel 4. 12** Summary Tahap 1-4 Zero Entry Hacking (ZEH).....136
**Tabel 5. 1** Identifikasi Kerentanan .....138
**Tabel 5. 2** Pengukuran Kerentanan dengan CVSS.....140

# DAFTAR LAMPIRAN

**Lampiran 1** Surat Pernyataan Perjanjian Kerahasiaan Penetration Test .....159
**Lampiran 2** Surat Pernyataan Perjanjian Kerahasiaan Penetration Test .....160
**Lampiran 3** Surat Persetujuan Penelitian .....161
**Lampiran 4** Surat Permohonan Penelitian.....162
**Lampiran 5** Hasil Wawancara dengan Bpk. Ardan.....163
**Lampiran 6** Hasil Wawancara dengan Bpk. Hafiz Diskominfo Tangerang Selatan .....163
**Lampiran 7** Flowchart Tahap Exploitation .....164

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Saat ini dunia sedang berada di era digital, dimana informasi sebagai tahap lanjutan dari era lainnya seperti pra sejarah, era agraris, dan era industri. Informasi menjadi semakin penting seiring dengan perkembangan teknologi yang begitu pesat. Pada tahun 2022, Badan Pusat Statistik (BPS) melakukan perhitungan Indeks Pembangunan TIK yang ketujuh dengan mengacu pada metodologi dari ITU pada publikasi *Measuring Information Society* 2016. Perhitungan Indeks Pembangunan TIK 2021 yang dilakukan pada tahun 2022, baik pada tingkat nasional maupun provinsi, dengan hasil yang diketahui pada skala 0-10. Indeks Pembangunan TIK di Indonesia pada tahun 2021 diketahui sebesar 5,76 yang mengalami peningkatan dari tahun 2020 yang hanya sebesar 5,59. Di tahun 2021, menurut subindeks penyusun Indeks Pembangunan TIK memiliki pola yang serupa dengan tahun sebelumnya. Nilai subindeks yang tertinggi adalah subindeks keahlian TIK sebesar 5,97, diikuti subindeks akses dan infrastruktur TIK sebesar 5,76, dan subindeks penggunaan TIK sebesar 5,66 (Badan Pusat Statistik, 2022).

Berdasarkan data di atas, dapat diartikan bahwa hal tersebut memiliki peran penting dalam kehidupan bagi setiap individu maupun organisasi. Seiring dengan meningkatnya kebutuhan manusia akan penggunaan teknologi informasi dan komunikasi, semakin tinggi pula ancaman yang dapat diterima. Meningkatnya lalu lintas internet tentunya membukakan jalan besar bagi para pelaku kriminal siber untuk melakukan penyerangan guna mendapatkan sebuah informasi dengan tujuan tertentu (Badan Pusat Statistik, 2022)

Berdasarkan data yang dipaparkan dalam Laporan Bulanan Publik berupa hasil *monitoring* keamanan siber Agustus 2022, diketahui terdapat 44.776.891 anomali trafik dengan jumlah anomali tertinggi yang terjadi pada

tanggal 3 Agustus 2022 sebesar 3.103.770. Laporan ini juga mengklasifikasikan anomaly seperti APT, *Denial of Service*, *Exploit*, *Information Gathering*, *Information Leak*, *Malware*, *Other*, *Trojan Activity*, *Web Application Attack* dengan angka tertinggi sebesar 24.448.343 atas *Malware* (Direktorat Operasi Keamanan Siber, 2022). Hal serupa juga disampaikan oleh Direktorat Tindak Pidana Siber Bareskrim Polri, pada periode 2018 hingga 2020 (Januari – April) dengan jenis kejahatan siber *Computer-related crime* dan *Computer crime* dengan total kasus masing – masing pada tahun 2018 sebesar 3842 kasus dan 518 kasus, kemudian pada tahun 2019 sebesar 3917 kasus dan 705 kasus, dan pada tahun 2020 sebesar 1572 kasus dan 252 kasus (Sachroni, S.H, 2020). Oleh karena itu, keamanan juga perlu ditingkatkan sebagai upaya untuk menghindari berbagai macam serangan yang mengancam sebuah sistem informasi atau sebuah jaringan. Kemajuan di era ini menuntut segalanya menjadi lebih praktis dengan harapan segala kegiatan bisnis, transaksi ataupun pertukaran data dapat berlangsung cepat tanpa adanya gangguan dari pihak manapun. Dalam hal ini gangguan yang mungkin datang dan tidak diinginkan adalah serangan dari peretas (*hacker)*. Oleh karena itu, keamaan jaringan atau sistem sangat perlu ditindak lanjuti sebagai bentuk antisipasi dari ancaman.

Keamanan jaringan adalah proses pencegahan dan pengidentifikasi pengguna yang tidak dikenal atau tidak sah dari suatu jaringan komputer. Keamanan jaringan juga disebutkan sebagai sistem yang sangat penting dalam upaya menjaga validitas dan integrasis sebuah sistem serta menjamin tersedianya layanan bagi pengguna (Hayaty, 2020). Keamanan jaringan memiliki tujuan untuk mengantisipasi kemungkinan resiko yang ada dalam bentuk ancaman secara fisik maupun *logic* baik langsung ataupun tidak langsung dalam sebuah jaringan. Berkaitan dengan hal ini, tujuan dari keamanan jaringan juga berarti mencegah penyusup yang masuk dengan menggunakan identitas legal (seseorang yang mempuyai otoritas) yang berhasil diretas dan digunakan untuk mengelabui sebuah sistem jaringan.

Dalam beberapa tahun terakhir *website* menjadi layanan yang sudah menjadi kebutuhan, karena mempermudah dan mempercepat penyebaran informasi. Tidak hanya itu, *website* juga digunakan oleh banyak bidang. Mulai dari segi bisnis, maupun perusahaan untuk membangun *profile* dan menyediakan pelayaan secara praktis baik pemerintahan maupun swasta. Dalam proses nya, masalah yang dialami dinilai berasal dari dalam maupu dari luar, sebagai contoh adalah serangan terhadap layanan yang bersumber dari internet (Tampubolon et al., 2021).

Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (PTSP) Kota Tangerang Selatan menjadi salah satu contoh instansi yang memaksimalkan penggunaan *website*. *Website* dari Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (PTSP) Kota Tangerang Selatan berisikan informasi penting bagi publik terkait perizinan berinvestasi. Hal ini menjadi penting, karena kemudahan yang diberikan kepada masyarakat luas dari penerapan *website* yang sedemikian rupa dan perlu dijaga keamanan sistemnya. Menanggapi masalah siber di era digital ini, Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dinilai cukup serius dalam hal kerentanan server dengan informasi yang didapatkan bahwa belum pernah terjadi peretasan pada server di instansi tersebut yang diketahui berdasarkan wawancara singkat penulis dengan salah satu penanggung jawab *website* yaitu Bapak Ardan, melalui media *online Whatsapp*.

Dari hasil wawancara singkat antara penulis dengan Bapak Ardan selaku pihak penanggung jawab *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, diketahui bahwa saat ini pihaknya sudah melakukan pengamanan dari sisi server dengan menggunakan *Honeypot* dan WAF (*Web Application Firewall*) dari BSSN. Berkaitan dengan hal tersebut, pada 25 Oktober 2021 Situs Pusat *Malware* milik BSSN diretas *hacker* menggunakan Teknik *defacement* berupa perubahan halaman muka yang bertuliskan "*Hacked by theMxonday"*. Hal ini menjadikan dasar alasan penulis untuk melakukan *Vulnerability Assessment* dan *Penetration Testing*, karena Situs Pusat *Malware* milik BSSN mampu diretas, dan berdasarkan hasil wawancara

tersebut diketahui bahwa keamanan *server* miliki Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dirancang oleh BSSN. Meskipun didapatkan informasi bahwa belum pernah terjadi peretasan, namun penulis berusaha untuk menguji dan mencari informasi apakah *website* dari Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan sudah aman sebagai langkah proaktif yang dapat dilakukan untuk meminimalisir kemungkinan terburuk yang dapat terjadi.

Indonesia memerlukan model dan pola pengelolaan informasi pada perspekstif *secure* dan *defense. Secure* memberikan kemampuna bagi seseorang atau kelompok untuk memberikan jaminan keamanan secara mandiri. Sedangkan *defense*, sumber daya yang ada dikelola secara aktif dengan menginisiasi model keamanan yang preventif (Riasetiawan, 2016). Dalam menghadapi ancaman siber, sangat disarankan bagi pihak-pihak yang bersangkutan untuk mematuhi regulasi keamanan yang berlaku, dengan melakukan monitoring terhadap suatu sistem dengan metode atau *tools* tertentu, salah satunya *Vulnerability* Assessment. *Vulnerability Assessment* dianggap memiliki capaian yang baik sebagai alat untuk memastikan keamanan siber dalam sebuah sistem (Sahtyawan, 2019).

Untuk memastikan kemanan siber pada sistem, *Vulnerability Assessment* sangat baik dilakukan sebagai dasar dari pengendalian secara preventif karena dapat mendefinisikan, mengidentifikasi, mengelompokkan, dan memprioritaskan keamanan pada sebuah sistem *web* (Mira Orisa & Ardita, 2021). Selain itu, *Vulnerability Assessment* bukan hanya melakukan pemindaian dari jaringan menggunakan *tools* terkait saja, hasil dari proses ini berbeda dari *pentest blackbox* dan *greybox*. Kedua *pentest* tersebut tidak mampu memaparkan hasil yang komprehensif karena potensi kerentanan kritis tidak seluruhnya teridentifikasi (Lumy, 2010).

Keamanan sebuah sistem informasi dapat dikatakan baik apabila memenuhi kriteria ataupun persyaratan keamanan komputer dan jaringan. Dalam hal ini, segitiga CIA (*Confidentiality, Integrity,* dan *Availability*),

*Authenticity*, dan *Accountability* dapat menjadi tolak ukur keamanan sistem yang baik (Janner Simarmata, Dimas Sasongko et al., 2022).

Berkaitan dengan hal ini, diperlukan upaya untuk melakukan pengukuran terkait kerentanan dari sebuah sistem melalui berbagai cara. Beberapa diantaranya adalah CVSS (*Common Vulnerability Scoring System*), CWE (*Common Weakness Enumeration*), OWASP (*Open Web Application Security Project*), NIST (*National Institute of Standards and Technology*), dan ISO/IEC 27001.

Dari beberapa *tools* yang dapat digunakan untuk melakukan pengukuran diatas, diketahui bahwa CVSS (*Common Vulnerability Scoring System*) telah menjadi aspek yang diperhatikan oleh keamanan sistem terkait upaya identifikasi karakteristik kerentanan dan tingkat keparahan melalui skor penilaian selama bertahun-tahun. Tidak hanya itu, *tools* ini banyak digunakan karena secara spesifik memberikan penyerdehanan skor penilaian kerentanan yang dapat memudahkan pengukuran (Pesona, 2022). CVSS (*Common Vulnerability Scoring System*) digunakan untuk mengetahui bagaimana dampak potensial akubat *vulnerability* yang akan dijadikan sebagai penilaian atas dasar kualitas sebuah kelemahan (Retna Mulya & Tarigan, 2018). Dari 66 jenis kerentanan vector CVSS (*Common Vulnerability Scoring System*) sebanyak 90% mewakili kerentanan yang diterbitkan oleh Database Kerentanan Nasional Amerika Serikat. Berisi tiga kelompok metrik: *base*, *temporal*, *environtmental*, yang membantu dalam upaya pemetaan tingkat kerentanan yang ditemukan (Mell et al., 2022).

*Vulnerability Assessment* erat kaitannya dengan *penetration testing* sebagai serangkaian proses yang dilakukan sebagai upaya evaluasi keamanan sebuah sistem dengan simulasi serangan. Terkait *penetration testing*, terdapat beberapa metode yang dapat digunakan yaitu, *black-box testing*, *white-box testing*, dan *grey-box testing* (Božić et al., 2019). Penggunaan metode ini diterapkan sesuai dengan kebutuhan. Dalam penelitian ini, pengujian bertujuan untuk dapat menemukan sebuah celah atau kesalahan dan memperbaiki kesalahan yang ada, sehingga pengujian hanya akan terbatas pada spesifikasi

fungsional tanpa menguji desain dan kode program. Atas hal ini, metode pengujian yang dimaksudkan adalah *black-box testing* (Murni & Zulham, 2022). Penelitian ini termasuk kedalam jenis pengujian *grey-box testing*, karena pengujian yang dilakukan dengan memanfaatkan beberapa informasi yang didapatkan oleh pihak terkait untuk kemudian dilakukan pengujian atau pengumpulan informasi lanjutan.

Peneliti dalam penelitian ini juga berlaku sebagai *pentester* atau bertindak sebagai seorang *hacker*. Terdapat beberapa jenis *hacker* seperti, *black hat, white hat* dan *grey hat*. Dalam penelitian ini, peneliti juga berperan sebagai *hacker* dengan jenis *white hat,* karena aktivitas yang dilakukan telah mendapatkan izin dan tujuannya adalah untuk mencari celah kerentanan yang ada untuk kemudian diberikan hasilnya kepada pihak yang berkepentingan (Cyber Academy Indonesia, 2022).

Sebagai serangkaian proses yang dilakukan untuk mengevaluasi permasalahan keamanan sistem, *vulnerability assessment* dan *penetration testing* digunakan dalam penelitian ini karena serangkaian proses yang dilakukan menggunakan metode ini dapat menemukan kerentanan yang berbaya untuk kemudian dilakukan pengujian terhadap kerentanan atau celah yang ditemukan, sehingga dapat dilakukan perbaikan pada kerentanan yang ditemukan sehingga kerentanan dapat dihilangkan (Khera et al., 2019).

Terdapat beberapa metodologi yang dapat digunakan utuk melakukan uji *penetration* testing seperti OSSTMM (*Open Source Security Testing Methodology Manual*), ISSAF (*Information System Security Assessment Framework*), dan lain sebagainya (Germanotta, 2021). Beberapa metode tersebut memiliki kelebihan dan kekurangan, serta langkahnya masing-masing, Namun, pada penelitian ini peneliti menggunakan metode *Zero Entry Hacking* dengan empat tahapan sederhana yaitu, Pengintai Sistem (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi Celah Keamanan (*Exploitation*), dan Pasca Eksploitasi (*Post Exploitation*) (P. Engebretson, 2013). Metode *Zero Entry Hacking* digunakan dalam penelitian ini sebagai metode *penetration*

*testing* karena memiliki tahapan sederhana dan sangat cocok untuk pemula (Pandapotan, 2021).

Hal ini merujuk pada beberapa penelitian sebelumnya yang menggunakan metode serupa dengan beberapa *tools* lainnya. Nur (2019) dalam penelitian yang berjudul "ANALISIS DAN PENGUJIAN KERENTANAN SISTEM INFORMASI PERPUSTAKAAN" menggunakan metode *zero entry hacking* dengan *tools SQL Injection* dan *Cookie Injection*. Selain itu, penelitian sebelumnya dengan judul "*Analysis and Impact of Vulnerability Assessment and Penetration Testing"* oleh (Khera et al., 2019), menggunakan *Vulnerability Assessment* dan *penetration testing* dengan *tools* OWASP TOP 10 seperti, *wire shark, Nmap, metaploit, air crack, injection*, dan lain sebagainya. Berkaitan dengan hal tersebut, penelitian ini menggunakan beberapa *tools* yang ditetapkan sesuai dengan kebutuhan yang diantaranya, Nmap, OWASP ZAP, Accunetix, dan Uniscan. Adapun pemilihan *tools* ini dilatar belakangi oleh beberapa penelitian sebelumnya yang diantaranya penelitian oleh Nur (2019) dan penelitian oleh Aliefyan (2020) terkait keakuratan hasil dari pengujian yang dilakukan. Selain itu, pemilihan *tools* ini juga disesuaikan dengan tahapan-tahapan yang ada pada *Zero Entry Hacking* sebagai metode *penetration testing* yang penulis gunakan.

Penelitian ini menggunakan jenis penelitian eksperimental dengan melalui beberapa tahapan pemindaian serta pengujian yang akan dilakukan dengan tahapan yang telah ditentukan oleh penulis. Beberapa penelitian sebelumnya dengan topik serupa yang berjudul '*Analysis and Impact of Vulnerability Assessment and Penetration Testing'* oleh Khera et al. (2019), dan 'PENGUJIAN KERENTANAN DAN PENETRASI KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ' oleh Listartha et al. (2021), melakukan pengujian dengan tahapan-tahapan yang ditentukan sesuai dengan metode yang digunakan pada masing-masing penelitian. Beberapa penelitian yang dijadikan sebagai acuan penulisan tersebut, menggunakan jenis penelitian eksperimen untuk memperoleh hasil dalam pengujiannya. Berdasarkan hal tersebut, penulis menggunakan

penelitian eksperimen sebagai jenis penelitian yang digunakan pada penelitian ini untuk mendapatkan hasil yang tepat.

Berdasarkan latar belakang yang telah diuraikan, maka penulis akan melakukan penelitian yang berjudul "***VULNERABILITY ASSESSMENT* DAN *PENETRATION TESTING* (VAPT) MENGGUNAKAN METODE *ZERO ENTRY HACKING* (ZEH*)* TERHADAP *WEBSITE* Studi Kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan**".

## 1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah yang diuraikan diatas maka berikut beberapa masalah yang di identifkasi:

1. Indeks Pembangunan TIK sejalan dengan semakin tingginya kasus serangan siber
2. Peretasan situs pusat *malware* miliki BSSN dapat mengindikasikan adanya kerentanan pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan karena *honeypot* yang dimiliki dipasangkan oleh BSSN.
3. *Vulnerability Assessment* dan *Penetration Testing* diperlukan sebagai sebuah langkah proaktif untuk menemukan kerentanan untuk kemudian dapat melakukan perbaikan.

## 1.3 Rumusan Masalah

Berdasarkan latar belakang dan Identifikasi masalah yang telah dikemukakan diatas, maka penulis merumuskan beberapa masalah yaitu:

1. Apa saja celah kerentanan pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dengan menggunakan Metode Penetrasi *Zero Entry Hacking*?
2. Bagaimana kondisi dan tingkat kerentanan sistem informasi pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan setelah dilakukan pemindaian dengan *Vulnerability Assessment tools* dan diukur menggunakan CVSS (*Common Vulnerability Scoring System*)?

## 1.4 Batasan Masalah

Sebagai pembatasan pengembangan penelitian dan alat untuk tetap fokus dan sesuai dengan tujuan penelitian yang ditetapkan, maka penulis memberikan ruang lingkup batasan sebagai berikut:

A. Metode

1. Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian eksperimen dengan menggunakan *Zero Entry Hacking* (ZEH) sebagai metode *penetration testing* tanpa *social engineering*. Hasil dari kerentanan yang ditemukan akan dianalisis tingkat kerentanannya melalui kalkulator berbasis *web Common Vulnerability Scoring System* (CVSS) https://www.first.org/cvss/ (FIRST, 2019).
2. Jenis *Penetration Testing* pada penelitian ini menggunakan metode *grey-box testing* karena peneliti mendapatkan beberapa informasi melalui narasumber atau pihak terkait untuk dapat membantu proses penelitian.
3. Penulis dalam penelitian ini berperan sebagai *hacker* dengan jenis *White Hat* atau *Ethical Hacker*, karena penulis mendapatkan izin untuk melakukan pengujian dan dilakukan dengan tujuan yang baik.
4. *Penetration Testing* yang dilakukan adalah *Penetration Testing External* untuk menemukan dan mengeksploitasi kerentanan sistem, karena hasil pengujian ini nantinya akan memberikan gambaran apakah tindakan keamanan yang diterapkan dapat dikatakan cukup baik untuk mengamakan data atau informasi yang ada.
5. *Penetration Testing* ini terbatas pada bentuk simulasi pengujian yang dilakukan dalam ruang lingkup *Network Penetration Testing*.

B. Proses

1. Penelitian ini akan melalui beberapa tahapan penelitian sesuai metode *Zero Entry Hacking*, dengan observasi dan wawancara sebagai langkah awal pengumpulan data, kemudian pengintaian server, pemindaian, dan *penetration* yang dilakukan pada aplikasi berbasis *web* milik Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, yaitu

https://dpmptsp.tangerangselatankota.go.id/ , yang penerapannya akan diserahkan secara penuh kepada kewenangan instasi terkait.

C. *Tools*

1. Penelitian ini menggunakan Kali Linux dalam pengujiannya,
2. *Whois,* digunakan untuk mencari alamat IP dan informasi berharga seperti pencatat *domain*, status, tanggal kadaluarsa, dan nama *server* DNS https://who.is .
3. *The Harvester*, versi 4.2.0 digunakan untuk mendapatkan informasi *email, subdomain, host, port,* dan lain sebagainya https://www.cybervie.com/blog/what-is-the-harvester/ .
4. *Whatweb,* versi 0.5.5 digunakan untuk mendapatkan alamat *email*, nomor versi, ID akun, modul kerangka kerja *web*, kesalahan SQL, dan lain sebagainya https://www.kali.org/tools/whatweb/ .
5. *CXSecurity,* digunakan sebagai panduan untuk melakukan identifikasi terkait objek yang di uji melalui informasi pada *Database* yang ada pada *CXSecurity https://cxsecurity.com/wlb/about/* .
6. *Google Hacking Database + Google Dorking,* digunakan untuk mencari sebuah informasi yang tidak mudah terlihat oleh publik untuk kemudian digunakan dalam menemukan kerentanan pada sebuah situs *web* https://www.exploit-db.com/google-hacking-database .
7. *Terminal,* pada penelitian ini *terminal* digunakan sebagai alat untuk melakukan perintah pengujian dari masing-masing *tools* yang digunakan dan melakukan *ping* https://help.ubuntu.com/kubuntu/desktopguide/id/terminals.html .
8. *Nmap,* versi 7.93 digunakan untuk melakukan *scanning port* dan untuk mendapatkan sistem operasi yang digunakan, jenis *firewall*/*filter* paket yang digunakan dan karakteristik lainnya dan untuk melakukan eksploitasi https://belajarlinux.id/cara-menggunakan-nmap-di-linux/ .
9. *OWASP ZAP*, versi 2.12.0 digunakan untuk menemukan kerentanan dan eksploitasi https://edysusanto.com/owasp-open-web-application-security-project-zap/ .

10. *Uniscan*, versi 6.3 digunakan untuk melakukan *vulnerability scanning* https://sourceforge.net/projects/uniscan/ .
11. *Acunnetix*, versi 13.0.200217097 digunakan untuk melakukan *vulnerability scanning* *https://www.linuxsec.org/2020/03/uniscan.html* .
12. *Weevely*, versi 4.0.1 digunakan untuk melakukan melakukan tindakan pasca eksploitasi dalam hal memelihara akses https://medium.com/@idfaris.official/backconnect-menggunakan-weevely3-di-ubuntu-73e1c435cbd5 .
13. *Burp Suite*, versi 2023.1.2 digunakan untuk melakukan eksploitasi berbasis *web* berdasarkan kerentanan yang telah didapat dari tahap sebelumnya https://ilmubersama.com/2021/02/22/hacking-lab-setup-burp-suite-di-kali-linux/ .

## 1.5 Tujuan Penelitian

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Mendapatkan celah kerentanan yang ada pada server *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dengan menggunakan Metode Penetrasi *Zero Entry Hacking*
2. Mendapatkan dan mengidentifikasikan kondisi serta tingkat kerentanan sistem informasi pada server *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan yang telah dilakukan melalui pemindaian dengan *Vulnerability Assessment tools* yang dan diukur menggunakan CVSS (*Common Vulnerability Scoring System*).

## 1.6 Manfaat Penelitian

Adapun manfaat yang didapatkan dari analisis keamanan *website* ini adalah sebagai berikut:

1. **Bagi Penulis**
   a. Untuk memenuhi salah satu syarat kelulusan Strata Satu (S1), Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta.
   b. Penulis dapat menerapkan pengetahuan yang diperoleh selama menjalani perkuliahan untuk memberikan solusi yang telah dipaparkan sebelumnya.
   c. Penulis dapat memperluas pengetahuannya tentang *Vulnerability Assessment* dan *Penetration Testing* (VAPT) dengan metode *Zero Entry Hacking* (ZEH) dan mengembangkannya untuk diterapkan ke sistem yang lebih besar dan menerapkannya pada keadaan di dunia nyata.
   d. Memahami bagaimana menangani isu keamanan pada *website* untuk mencegah penyusup atau peretas yang berusaha menyerang melalui celah kerentanan yang ada.

2. **Bagi Universitas**
   a. Mengetahui kemampuan mahasiswa dalam menerapkan dan mengembangkan ilmu yang di dapatkannya selama menjalani perkuliahan di kampus.
   b. Mengukur tingkat kemampuan Mahasiswa dalam menerapkan ilmu akademis maupun non-akademis di lingkungan masyarakat dan industri.
   c. Menjadi referensi baru bagi penelitian lain di bidang *Cyber Security* khususnya di keamanan sistem jaringan *website* di lingkup UIN Syarif Hidayatullah Jakarta.

3. **Bagi Intansi Terkait**
   a. Sebagai acuan untuk bahan evaluasi keamanan sistem informasi.
   b. Data yang disajikan dapat diguakan untuk meningkatkan keamanan sistem informasi.
   c. Mencegah terjadinya serangan terhadap website.

4. **Bagi Masyarakat**
   a. Menambah pengetahuan tentang keamanan sistem informasi.
   b. Membantu masyarakat untuk mendapatkan karya tulis terpercaya.
   c. Sebagai acuan atau referensi untuk penelitian sebelumnya.

## 1.7 Metodologi Penelitian

### 1.7.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah studi pustaka dan studi lapangan. Studi pustaka dilakukan dengan mencari informasi dari berbagai sumber seperti buku, *e-*book, *web,* dan studi literatur sejenis. Sedangkan studi lapangan menggunakan observasi dan wawancara.

### 1.7.2 Metode Pengujian dan Analisis

Penelitian ini merupakan penelitian eksperimental dengan menggunakan *Zero Entry Hacking* (ZEH) sebagai metode dalam melalukan pengujian dan analisis. Metode *Zero Entry Hacking* (ZEH) ini memiliki 4 tahapan sebagai berikut (Sahtyawan, 2019).

1. Pengintaian Target (*Reconnaisance*), dilakukan dengan menggunakan *tools Whatweb, Whois, TheHarvester, CXSecurity, Google Hacking Database + Google Dorking*
2. Pemindaian (*Scanning*), dilakukan dengan menggunakan *tools Nmap, OWASP ZAP, Uniscan, dan Acunetix*.
3. Eksploitasi (*Exploitation*), pada tahap ini *tools* yang digunakan antara lain *Burp Suite.*
4. Pasca Eksploitasi (*Post Exploitation*), pada tahap ini *tools* yang digunakan adalah *Weevely*.

### 1.7.3 Jenis Penelitian

Penelitian ini menggunakan jenis penelitian eksperimen *Pre-Experimental Design* dengan jenis *One Shot Case Study* karena pada

penelitian ini hanya terdapat satu kelompok yang diberikan *treatment* atau perlakuan dan tidak ada kelompok pembanding. Adapun tahapan yang akan dilakukan pada penelitian ini antara lain sebagai berikut.

1. Tahap Persiapan

   Perancangan eksperimen meliputi bentuk penelitian eksperimen dan desain yang akan digunakan, studi pustaka, dan lain sebagainya.
2. Pelaksanaan Penelitian

   Pada tahap ini, penelitian akan berlangsung dengan menggunakan metode pengujian *Zero Entry Hacking* dalam melakukan *penetration testing*.
3. Pengolahan dan Analisis data

   Hasil dari eksperimen akan diinterpretasikan melalui tabel kerentanan yang sebelumnya telah diukur menggunakan *Common Vulnerability Scoring System* (CVSS).

## 1.8 Sistematika Penulisan

Sistematika yang dibuat pada tugas akhir ini akan dibagi dalam enam bagian yaitu :

**BAB I PENDAHULUAN**

Dalam bab ini membahas mengenai latar belakang penulisan perumusan masalah, Batasan masalah, tujuan dan manfaat , metode, dan sistematika penulisan yang merupakan gambaran menyeluruh dari penulisan skripsi ini.

**BAB II LANDASAN TEORI**

Dalam bab ini membahas mengenai berbagai teori yang mendasari analisis permasalahan pada pembahasan

**BAB III METODOLOGI PENELITIAN**

Bab ini berisi pembahasan atau pemaparan metode yang dipakai oleh penulis dalam pencarian data maupun perancangan sistem dan eksperimen yang akan dilakukan di penelitian.

**BAB IV ANALISIS DAN IMPLEMENTASI SISTEM**

Bab ini membahas mengenai hasil dari Analisa dan implementasi sistem selama penelitian ini berlangsung.

**BAB V HASIL DAN PEMBAHASAN**

Bab ini berisi hasil dan pembahasan yang didapat dari penelitian yang dilakukan.

**BAB VI PENUTUP**

Pada bab ini kesimpulan dari hasil pembahasan seluruh bab serta saran-saran yang mungkin dapat diperhatikan serta dipertimbangkan untuk pengembangan sistem yang lebih baik di masa yang akan datang.

# BAB II
# LANDASAN TEORI

## 2.1 Konsep Dasar Sistem

### 2.1.1 Pengertian Sistem

Suatu sistem dapat didefinisikan sebagai sekumpulan atau himpunan unsur, komponen, atau variabel yang teroganisir, saling berinteraksi, memiliki ketergantungan antara satu dengan yang lainnya, dan terpadu. Sebuah sistem sendiri terdidi atas berbagai komponen terpadu untuk mencapai satu tujuan. Model dasar dari bentuk sistem ini adalah adanya masukan, pengolahan, dan keluaran yang memiliki cara pandang dengan mensyaratkan suatu pelaksanaan pekerjaan secara integratif baik melibatkan manusia, perkakas, metode, maupun sumber daya yang dimanfaatkan (Sutabri, 2012).

Gordon B. Davis dalam modul Konsep Dasar Sistem Informasi (Kusnendi, M. S., & Modul, 2017) menyatakan, bahwa sistem dapat berupa abstrak atau fisik. Sistem abstrak adalah susunan yang teratur dari gagasan atau konsepsi yang saling bergantung. Sedangkan sistem yang bersifat fisik adalah serangkaian unsur yang teratur dari gagasanan tentang Tuhan, manusia, dan lain sebagainya. Kemudian pernyataan lainnya dipaparkan oleh Norman L. Enger yang menyebutkan bahwa sistem dapat terdiri atas kegiatan-kegiatan yang berhubungan dalam rangka untuk mencapai sebuah tujuan.

Sistem adalah suatu kesatuan yang terdiri dari dua atau lebih komponen atau subsistem yang berinteraksi untuk mencapai suatu tujuan. Interaksi antara subsistem yang sedemikian rupa ini, akan

membentuk satu kesatuan yang terpadu dan terintegrasi (*integrated*) (Heartly, 2003).

### 2.1.2 Karakteristik Sistem

Buku Konsep Sistem informasi oleh Tata Sutabri (Sutabri, 2012) menjelaskan bahwa model sebuah sistem secara umum adalah *input*, proses, dan *output*. Hal tersebut merupakan konsep yang sangat sederhana dari sebuah sistem karena sebuah sistem dapat memiliki beberapa banyak masukan dan keluaran. Selain itu, sebuah sistem juga memiliki karakteristik atau sifat-sifat tertentu yang mendeskripsikan bahwa suatu hal tersebut dapat dikatakan sebagai sebuah sistem. Adapun karakteristik yang dimaksud adalah sebagai berikut:

1. Komponen Sisten (*Components*)

   Suatu sistem terdiri atas sejumlah komponen yang saling beriteraksi satu sama lain, artinya sejumlah kompinen ini saling bekerja sama dan membentuk satu kesatuan. Komponen-komponen ini dapat berupa suatu bentuk subsistem. Setiap subsite mini memiliki sifat dari sistem yang menjalankan suatu fungsi tertentu dan mempengaruhi proses sistem secara menyeluruh. Suatu sistem nantinya dapat mempunyai sistem yang lebih besar atau dapat juga disebut sebagai "supra sistem".

2. Batasan Sistem (*Boundary*)

   Ruang lingkup sistem merupakan daerah yang membatasi antara sistem dengan sistem yang lain atau sistem dengan lingkungan luarnya. Batasan ini memungkinkan suatu sistem dinilai sebagai satu kesatuan yang tidak dapat dipisahkan.

3. Lingkungan Luar Sistem (*Environtment*)

Segala bentuk diluar ruang lingkup atau batasan sistem yang memberi pengaruh pada operasi sistem tersebut diketahui sebagai lingkungan luar sistem. Lingkungan luar sistem ini dapat menguntungkan dan dapat juga merugikan sistem itu sendiri. Atas hal ini, lingkungan luar harus terjaga dan dipelihara. Lingkungan luar harus berada dalam kendali, sehingga lingkungan luar yang merugikan dapat dikendalikan untuk menghindari terganggunya kelangsungan hidup sistem tersebut.

4. Penghubung Sistem (*Interface*)

   Media yang menghubungkan sistem dengan subsistem lain disebut sebagai penghubung sistem atau *interface*. Penghubung ini memungkinkan segala sumber daya mengalir dari satu subsistem ke subsistem yang lainnya. Bentuk *output* dari satu subsistem akan menjadi *input* bagi subsistem lain melalui penghubung atau *interface*. Hal ini menjadi dasar agar sistem dapat terintegrasi dan membentuk satu kesatuan.

5. Masukan Sistem (*Input*)

   Energi yang dimasukkan ke dalam sistem disebut masukkan sistem. Masukkan sistem ini dapat berupa pemeliharaan (*maintenance input*) dan sinyal (*signal input*). Sebagai contoh, di dalam suatu unit sistem komputer, program adalah *maintenance input* yang digunakan untuk mengoperasikan komputer dan data adalah *signal input* untuk diolah menjadi informasi.

6. Keluaran Sistem (*Output*)

   Hasil yang didapat dan diklasifikasikan menjadi keluaran yang berguna. Keluaran ini merupakan masukan bagi subsistem yang

lain seperti sistem informasi. Hasil dari proses ini adalah informasi yang digunakan sebagai masukkan dalam pengambilan keputusan atau hal-hal lain yang menjadi *input* bagi subsistem lain.

7. Pengolah Sistem (Proses)
   Sistem dapat mempunyai suatu proses yang akan mengubah *input* menjadi *output*. Contoh pengolahan sistem ini antara lain adalah pengolahan data, pelaporan perizinan dan non perizinan.

8. Sasaran Sistem (*Objective*)
   Suatu sistem memiliki tujuan dan sasaran yang pasti serta bersifat *deterministic*. Jika sistem tidak memiliki sasaran maka operasi sistem tidak ada gunanya. Suatu sistem dikatakan berhasil jika sasaran atau tujuan yang telah direncanakan dapat dicapai.

Karakteristik sistem ini digunakan sebagai landasan pengetahuan bagi peneliti untuk mengetahui bagaimana nantinya sebuah sistem ini bekerja, untuk kemudian peneliti dapat melakukan tahap-tahap penelitian yang peneliti tentukan.

## 2.2 Konsep Dasar Informasi

### 2.2.1 Pengertian Informasi

Menurut Jogiyanto informasi adalah hasil dari pengelolahan data dalam suatu bentuk yang jauh lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian-kejadian (*event*) yang nyata (*fact*) yang digunakan untuk pengambilan keputusan.

Kemudian pendapat lain dikemukakan oleh Kenneth C. Laudon bahwa informasi adalah data yang sudah dibentuk ke dalam format yang memiliki arti bagi manusia. Data yang dimaksud adalah sekumpulan baris fakta yang mewakili peristiwa yang terjadi pada organisasi atau pada lingkungan fisik sebelum diolah ke dalam suatu format yang dapat dipahami dan digunakan orang banyak (Kusnendi, M. S., & Modul, 2017).

Informasi juga dapat diartikan sebagai hasil dari pemrosesan data berupa fakta-fakta atau angka-angka yang bermanfaat bagi pengguna dalam melakukan analisis dan dasar pengambilan keputusan (Maulana, 2019). Selain itu juga disebutkan informasi merupakan sebuah data yang telah diolah sedemikian rupa sehingga dapat meningkatkan pengetahuan penerimanya (Muhamad Mawahib, 2015)

Berdasarkan beberapa penjelasan di atas, artinya sebuah informasi memiliki peran yang sangat penting. Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan sebagai instansi yang memberikan pelayanan informasi melalui *website* tentunya memiliki informasi yang sangat penting karena berkaitan dengan pelayanan yang diberikan bagi masyarakat.

### 2.2.2 Nilai dan Kualitas Informasi

Nilai dari sebuah informasi yang dimuat dalam buku Konsep Sistem Infornasi oleh Tata Sutabri (Sutabri, 2012) menjelaskan bahwa nilai tersebut ditentukan oleh 2 (dua) hal, yaitu manfaat dan biaya untuk mendapatkannya. Informasi ini dapat dikatakan bernilai apabila manfaat yang diberikan lebih besar dibandingkan biaya yang dikeluarkan untuk mendapatkannya. Pengukuran nilai informasi didasrkan atas 10 (sepuluh) sifat, yaitu:

a. Mudah diperoleh
b. Luas dan lengkap

c. Ketelitian
d. Kecocokan
e. Ketepatan waktu
f. Kejelasan
g. Keluwesan
h. Dapat dibuktikan
i. Tidak ada prasangka
j. Dapat diukur

Kualitas dari suatu informasi diketahui berdasarkan 3 (tiga) hal, yaitu: informasi yang disajikan harus akurat (*accurate*), tepat waktu (*timeline*), dan relevan (*relevance*) yang akan dijabarkan sebagai berikut.

1. Akurat (*accurate*)

   Informasi harus bebas dari sesuatu yang salah dan menyesatkan. Informasi juga harus jelas mencerminkan maksud dan tujuan mengapa informasi tersebut harus disampaikan agar tidak terjadi gangguan yang menyebabkan rusaknya informasi tersebut.

2. Tepat Waktu (*timeline*)

   Informasi seharusnya tidak terlambat untuk disampaikan, karena informasi yang sudah lama atau terlambat tidak akan mempunyai nilai lagi karena informasi juga digunakan dalam upaya pengambilan keputusan. Jika keterlambatan terjadi dapat menimbulkan akibat yang fatal bagi sebuah organisasi atau pihak bersangkutan yang menggunakan sebuah informasi tersebut.

3. Relevan (*relevance*)

   Informasi tentunya mempunyai manfaat bagi penggunanya. Kebutuhan informasi yang relevan bagi setiap orang itu berbeda-beda, sehingga tiap informasi itu tertuju kepada setiap orang dengan kebutuhannya masing-masing.

Berdasarkan penjelasan di atas, nilai dan kualitas informasi menjadi salah satu aspek untuk mengetahui betapa pentingnya sebuah informasi atau data yang memenuhi kriteria tersebut. Dan beberapa kriteria, peneliti jadikan sebagai acuan untuk menilai apakah informasi yang disajikan oleh Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan telah memenuhi kriteria dari Nilai dan Kualitas Informasi.

## 2.3 Konsep Dasar Keamanan Sistem Informasi

### 2.3.1 Konsep Dasar Keamanan

#### 2.3.1.1 Pengertian Keamanan

Dalam KBBI Daring, pengertian aman adalah bebas dari bahaya atau ancaman, bebas dari gangguan (pencuri, hama, dan sebagainya), terlindung atau tersembunyi (tidak dapat diambil orang) (Kbbi, n.d.).

Secara umum terdapat 3 hal dalam konsep keamanan jaringan, yaitu:

1. Resiko atau tingkat bahaya (*risk*)

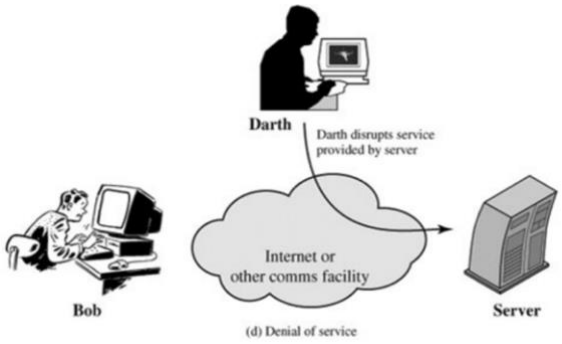
   Hal ini menyatakan seberapa besarnya kemungkinan penyusup berhasil atau mampu mengakses komputer dalam suatu jaringan.
2. Ancaman (*threat*)

   Menyatakan ancaman yang datang untuk memperoleh akses ilegal ke dalam suatu jaringan komputer yang seolah-olah mempunyai wewenang atas suatu jaringan tersebut.
3. Kerapuhan sistem

   Menyatakan seberapa mampu sistem keamanan dari sebuah jaringan yang dimiliki untuk mencegah akses

ilegal yang berusaha di dapatkan oleh seseorang dari luar terhadap jaringan tersebut (Suyuti Ma'sum et al., 2017).

Beberapa hal terkait pengklasifikasian serangan terhadap keamanan dikemumukan oleh William Stallings dalam bukunya yang berjudul "*Cryptography and Network Security*" menyebutkan bahwa cara yang berguna untuk mengklasifikasikan serangan keamanan adalah serangan dalam bentuk pasif dan serangan dalam bentuk aktif. Serangan pasif sendiri disebutkan sebagai upaya untuk mencoba dan mempelajari atau menggunakan informasi dari suatu sistem tetapi tidak mempengaruhi sumber daya sistemnya. Sedangkan serangan secara aktif disebutkan sebagai upaya untuk mengubah sumber daya sistem atau dengan kata lain mempengaruhi proses berjalannya sebuah sistem (Stallings, 2005). Pada serangan secara pasif, *hacker* memiliki tujuan untuk mendapatkan sebuah informasi yang sedang di transmisikan. Adapun dua jenis serangan pasif



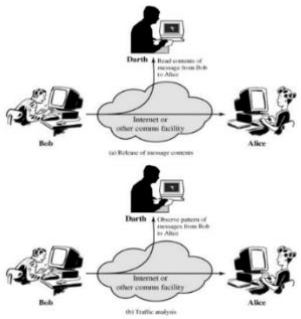

Gambar 2. 1 Serangan Secara Pasif

ialah pelepasan isi pesan dan analisis lalu lintas. Di dalam bukunya, William Stalling memberi penggambaran untuk model serangan secara pasif sebagai berikut:

Serangan secara pasif tidak melibatkan perubahan data sehingga sulit untuk dideteksi. Karena pada saat transfer data, pengirim dan penerima sebuah informasi akan tetap

merasa normal tanpa mengetahui bahwa pihak ketiga telah membaca isi pesan tersebut. (Stallings, 2005). Karena sulit untuk mendeteksi hal tersebut, tindakan terbaik yang dapat dilakukan adalah dengan melakukan pencegahan daripada mendeteksi.

Serangan ini memiliki target tertentu; seperti pada gambar, suatu entitas dapat menyembunyikan semua pesan diarahkan ke tujuan tertentu (misalnya, layanan audit keamanan). Bentuk lainnya adalah gangguan seluruh jaringan, baik dengan menonaktifkan jaringan atau dengan membebaninya sehingga kinerja menurun.




Gambar 2. 2 Serangan Secara Aktif
(Denial of Service)

Serangan secara aktif menjadi sulit dicegah berbeda dengan serangan secara pasif. Hal ini sebagai akibat dari potensi fisik, perangkat lunak, dan kerentanan jaringan.

Keamanan adalah sebuah upaya yang dilakukan untuk melindungi setiap orang, kelompok, lingkungan, serta keberadaan bumi itu sendiri. Pemikiran yang dikembangkan terkait keamanan oleh Buzan dan Hansen (2009) menjelaskan bahawa keamanan tidak hanya terkait pada memiliki perasaan terancam, namun juga upaya untuk menyerang dan mendominasi (Azizah, 2020). Pengertian keamanan juga disampaikan oleh Seth T. Ross (1999) bahwa

keamanan adalah sebuah kemampuan sistem untuk dapat melindungi informasi dan sumber daya sistem sehubungan dengan kerahasiaan dan integritas (Reza, 2020).

Berdasarkan beberapa pengertian di atas, dapat disimpulkan bahwa keamanan adalah sebuah upaya yang dilakukan untuk melindungi diri, sistem yang terintegrasi, dan lain sebagainya dari berbagai ancaman yang dapat mengganggu dan merusak. Dan kaitannya dengan penelitian ini adalah untuk mengetahui konsep dasar dari keamanan sistem dan bagaimana sebuah serangan dilakukan untuk kemudian mampu peneliti terapkan pada penelitian ini.

#### 2.3.1.2 Parameter Keamanan

Kejahatan komputer dalam risiko keamanan jaringan dapat digolongkan dari yang paling berbahaya hingga kejahatan yang *annoying* untuk memenuhi keinginan si penyerang. Atas hal ini, sistem keamanan perlu ditingkatkan sebagai upaya pencegahan dalam sistem pengamanan. Menurut Raharjo (2002), dalam teknologi komputer keamanan dapat diklasifikasikan menjadi empat, yaitu (Janner Simarmata, Dimas Sasongko et al., 2022):

1. Keamanan fisik (*physical security*)

   Keamanan dalam hal ini berfokus kepada dunia luar termasuk akses pihak-pihak yang berkaitan dengan peralatan dan media yang digunakan. Keamanan dalam hal ini ditujukan untuk melindungi dan mencegah terjadinya hal yang tidak diinginkan pada perlatan komputer dan sebagainya.
2. Keamanan yang berhubungan dengan orang (*personal security*)

Keamanan ini berkiatan dengan identifikasi dan profil risiko dari pihak-pihak yang mempunya akses. Dalam beberapa hal, sering kali celah keamanan sistem informasi bergantung pada pihak-pihak tersebut.

3. Keamanan data (*data security*)

   Keamanan yang termasuk didalamnya adalah kelamahan sistem yang digunakan dalam proses mengelola data, mencakup hal-hal terkait bagaimana data itu disimpan, apakah data tersebut dapat diakses oleh pihak lain, apakah data tersebut dapat terhapus dan termodifikasi.

4. Keamanan operasi (*operational security*)

   Keamanan ini merupakan prosedur yang diberlakukan untuk mengatur dan mengelola sistem keamanan. Keamanan dalam hal ini juga berarti melihat kepada ada atau tidaknya celah yang dapat disusupi kedalam sebuah sistem oleh penyusup atau pihak luar dengan kepentingan tertentu.

Beberapa penjabaran di atas, memberikan pengertian bahwa terdapat beberapa kondisi atau parameter yang harus dipenuhi untuk dapat dikatakan aman. Untuk itu, *point-point* penjelasan tersebut dapat peneliti jadikan sebagai acuan terkait keamanan dari *website* yang akan di teliti.

### 2.3.2 Keamanan Sistem Informasi

Keamanan sistem informasi merupakan hal yang perlu diperhatikan saat membangun sebuah sistem informasi. Keamanan sistem informasi ini digunakan terkait kebutuhan untuk menghindari adanya penyerangan yang dilakukan oleh pihak luar untuk mendapatkan akses masuk ke dalam sistem (Perdana, 2018). Keamanan sistem informasi terdiri atas perlindungan harian yang disebut sebagai keamanan informasi (*information security*) dan

segala bentuk persiapan operasionalnya. Keamanan sistem informasi berdasarkan apa yang disampaikan oleh G. J. Simons adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, setidaknya mampu mendeteksi adanya penyimpangan terhadap akses dan lain sebagainya dalam sebuah sistem informasi. Keamanan sistem informasi membagi dimensi menjadi tiga komponen yang dikenal sebagai *knowledge* (pengetahuan), *attitude* (sikap), dan *behavior* (perilaku seseorang) (Nurul et al., 2022).

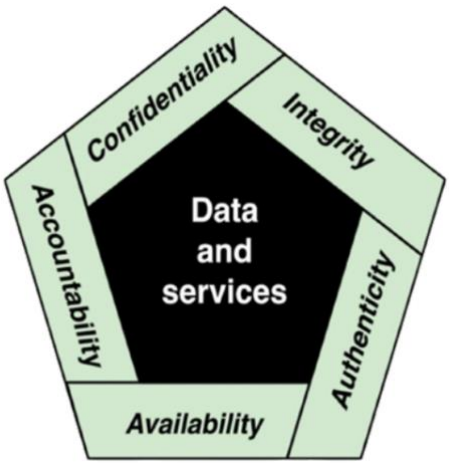
Keamanan informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, dan teknologi (Matin et al., 2018)

Berdasarkan penjelasan di dalam buku sistem keamanan data (Janner Simarmata, Dimas Sasongko et al., 2022), tujuan dari keamanan sistem informasi ini untuk mencapai keberhasilan sebuah sistem dalam menjaga *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) sumber daya sistem informasi secara menyeluruh.

Gambar 2. 3 Segiti CIA

Meskipun penerapan segitiga CIA (*Confidentiality, Integrity, Availability*) dapat dikatakan sudah cukup baik dalam menentukan tujuan dari sistem keamanan, beberapa pendapat lain berupa tambahan untuk menyajikan gambaran lengkap tentang bagimana keamanan secara lengkap disebutkan oleh beberapa ahli

yaitu *Authenticity* (keaslian) dan *Accountability* (akuntabilitas), seperti pada Gambar 2.4.




Gambar 2. 4 Persyaratan Keamanan Komputer dan Jaringan

#### 2.3.2.1 *Confidentiality* (Kerahasiaan)

Kerahasiaan berarti menjaga informasi ataupun data dari semua orang selain pihak-pihak yang memiliki hak terhadapnya. Informasi rahasia dalam hal ini meliputi (Sulistyowati S.Kom., M.MT., 2021):

a. Data pribadi.
b. Kekayaan intelektual bisnis.
c. Keamanan nasional negara dan pemerintah.

Aspek ini menjadi hal yang sangat penting untuk menjamin kerahasiaan data atau informasi dari pihak luar yang tidak memiliki hak atas data yang dikirim, diterima dan disimpan (Chazar, 2017). Berdasarkan beberapa penjelasan diatas, dapat disimpulkan bahwa aspek *confidentiality* (kerahasiaan) adalah hal penting yang diperlukan oleh sebuah sistem untuk dapat mencapai tingkat keamanan yang baik dalam hal informasi dan data penting bagi pengguna atau institusi terkait, dalam setiap proses yang dilakukan

baik mengirim, menerima dan menyimpan data atau informasi tersebut. Contoh pelanggaran dari aspek *confidentiality* (kerahasiaan) ini adalah seorang *hacker* atau penyusup yang berupaya untuk mendapatkan otorisasi terhadap suatu sistem dengan berbagai macam cara untuk mencapai tujuannya.

#### 2.3.2.2 *Integrity* (Integritas)

Aspek *integrity* erat kaitannya dengan aspek kerahasiaan sebagai langkah lanjutan untuk memastikan bahwa informasi yang telah ada tidak dapat diubah oleh pihak yang tidak memiliki wewenang atas hal tersebut dengan cara yang tidak dapat dideteksi (Reza, 2020). Bagi beberapa pihak, data dan informasi merupakan aset yang bersifat intelektual property. Sebagai contoh adalah berbagai subyek yang termasuk ke dalam kelompok hak cipta, paten, formulasi rahasia, dan database pelanggan.

Berbagai informasi penting ini dapat memiliki nilai yang besar. Oleh karena itu, perubahan yang terjadi terutama disebabkan oleh tindak pelanggaran yang dilakukan oleh pihak yang tidak memiliki hak atas hal tersebut dapat merusak nilai dan maknanya (Sulistyowati S.Kom., M.MT., 2021).

Secara singkat, aspek *integrity* (integritas) berarti mampun menjamin konsistensi terhadap data atau informasi beserta keasliannya. Hal ini akan mempermudah pihak yang berwenang untuk mengetahui upaya dari pihak luar untuk melakukan perubahan terhadap data atau informasi tersebut secara cepat dan tepat.

#### 2.3.2.3 *Availability* (Ketersediaan)

*Availability* (ketersedian) yang dimaksudkan dalam hal ini adalah mampu menjamin bahwa data tersedia saat dibutuhkan, dan dapat memastikan pihak yang memiliki hak atas akses tersebut dapat menggunakan informasi atau data terkait (Agustina et al., 2015). Dalam konteks keamanan informasi, ketersediaan umunya dinyatakan sebagai jumlah waktu pengguna dapat menggunakan sistem, aplikasi, dan data. Pengukuran waktu ketersediaan secara umum meliputi beberapa hal seperti, *uptime*, waktu henti (*down-time*), ketersediaan (*availability*), *mean time to failure* (MTTF), *mean time to repair* (MTTR), *mean time between failures* (MTBF), *recovery time objective* (RTO) (Sulistyowati S.Kom., M.MT., 2021).

#### 2.3.2.4 *Authenticity* (Keaslian)

Aspek tambahan ini mengacu pada orisinalitas informasi yang seharusnya tidak diubah oleh orang lain. *Authenticity* (keaslian) dalam informasi adalah kualitas atau keadaan asli bukan reproduksi atau fabrikasi. Informasi menjadi otentik Ketika dalam keadaan yang sama dimana ia dibuat, ditempatkan, disimpan, atau ditransfer. Hal ini berarti memverifikasi bahwa pengguna setiap masukan terhadap sistem berasal dari sumber yang terpercaya (Janner Simarmata, Dimas Sasongko et al., 2022).

#### 2.3.2.5 *Accountability* (Akuntabilitas)

Tujuan dari keamanan dengan persyaratan untuk tindakan oleh suatu entitas untuk dilacak secara unik ke entitas itu, sehingga kemudian hal ini mendukung *non repudiation*, pencegahan, isolasi kesalahan, deteksi instrusi

dan pencegahan, dan pemulihan setelah tindakan dan tindakan hukum.

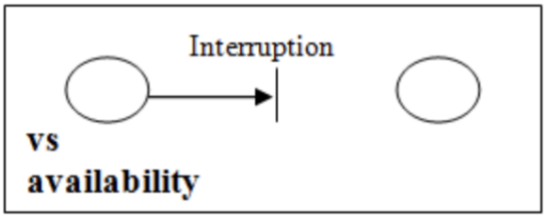
Karena sebuah sistem yang benar-benar aman belum menjadi tujuan yang dapat dicapai, kita harus dapat melacak pelanggaran keamanan terhadap pihak yang bertanggung jawab. Sistem ini harus menyimpan catatan aktivitasnya untuk memungkinkan analisis di kemudian hari untuk melacak pelanggaran keamanan atau untuk membantu dalam perselisihan transaksi (Janner Simarmata, Dimas Sasongko et al., 2022).

Segitia CIA dalam hal ini akan menjadi aspek-aspek yang dijadikan tolak ukur dalam penelitian ini terkait keamanan pada *website* yang diuji, sehingga dapat diketahui secara baik sejauh mana keamanan yang telah diterapkan dapat mengamankan sebuah *website*.

### 2.3.3 Tipe-tipe Ancaman Keamanan

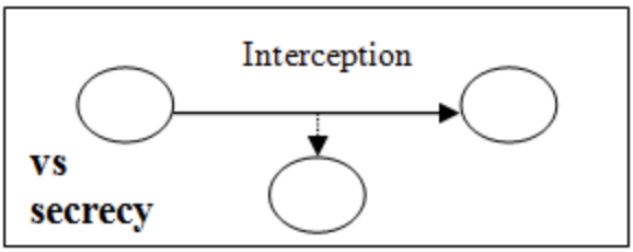
Ancaman keamanan didefinisikan sebagai *output* yang tidak diharapkan terkait pelanggaran keamanan informasi sebagai tindakan yang tidak terotorisasi. Tipe-tipe risiko ancaman keamanan dibagi menjadi empat jenis yaitu (Permatasari, 2016):

1. *Interruption*: Ancaman yang dimaksudkan adalah ancaman terhadap *availability*, yaitu data dan informasi dalam sistem yang dirusak dan dibuang atau dihapus sehingga tidak ada dan tidak berguna.



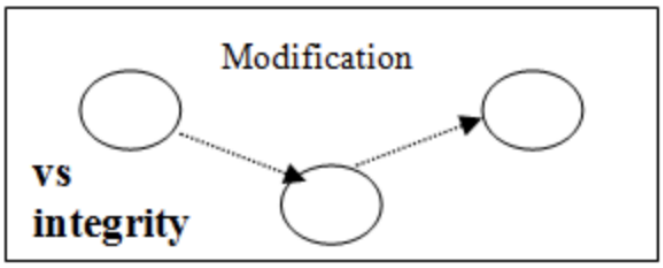

Gambar 2. 5 Interupsi

2. *Interception*: Merupakan ancaman terhadap *secrecy*, artinya orang yang tidak memiliki wewenang atau hak terhadap akses informasi pada sistem.



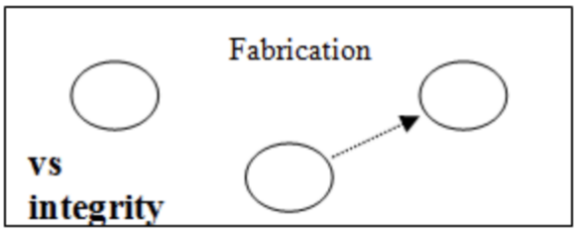

Gambar 2. 7 Intersepsi

3. *Modification*: Merupakan ancaman terhadap integritas, yaitu orang yang tidak berwenang tidak hanyak berhasil mendapatkan akses, tetapi juga dapat melakukan pengubahan terhadap informasi yang ada.




Gambar 2. 6 Modifikasi

4. *Fabrication*: Merupakan ancaman atas adanya pihak yang tidak berwenang untuk meniru atau memalsukan suatu objek ke dalam sistem.




Gambar 2. 8 Fabrikasi

Tipe-tipe keancaman di atas, dapat memberikan gambaran bagi peneliti terkait bagaimana ancaman yang dapat dilakukan

terhadap sebuah sistem. Sehingga, nantinya dapat peneliti manfaatkan sebagai dasar dari tahap pengujian yang akan peneliti lakukan.

### 2.3.4 Kerentanan Sistem

#### 2.3.4.1 Kerentanan (*Vulnerability*)

Kerentanan didefinisikan sebagai setiap kelemahan yang dapat di eksploitasi dan berdampak pada terganggunya sebuah sistem atas data atau sebuah informasi didalamnya (Kusnanto, 2016).

Di dalam buku *Computer Secutiy* Basics oleh kerentanan adalah titik di mana sistem rentan terhadap serangan. ancaman adalah kemungkinan bahaya bagi sistem. Bahayanya mungkin seseorang (cracker sistem atau mata-mata), benda (alat yang rusak), atau peristiwa (kebakaran atau banjir) yang mungkin mengeksploitasi kerentanan sistem. Semakin banyak kerentanan yang Anda lihat di sistem Anda, dan semakin banyak ancaman yang Anda yakini ada di luar sana, semakin hati-hati Anda perlu mempertimbangkan cara melindungi sistem Anda dan informasinya. Teknik untuk melindungi sistem Anda disebut penanggulangan.

Di dalam sebuah sistem, berbagai kerentanan mungkin saja ditemukan. Hal ini sebagai pengaruh dari masih rendahnya kesadaran pengguna atau sebuah sistem yang dibuat terkait keamaan siber yang berdampak pada kerentanan keamanan siber itu sendiri. Berbagai kerentanan yang tidak dapat dikendalikan akan merugikan berbagai pihak yang terlibat atau menggunakan sebuah sistem tersebut. Penjabaran ini dapat memberikan pemahaman kepada peneliti dan pihak-pihak terkait tentang bagaimana

kerentanan dapat memberikan dampak yang sedimikian rupa merugikan bagi berbagai pihak.

#### 2.3.4.2 Macam-macam Serangan terhadap Sistem

Serangan jaringan (*hacking*) adalah serangan yang dilakukan terhadap jaringan komputer yang terhubung dengan internet. Hal ini menyebabkan sebuah jaringan yang terdampak akan mengalami malfungsi dan berdampak besar terhadap sistem pada komputer maupun server yang diserang. Adapun berbagai macam serangan yang secara umum dilakukan terhadap jaringan komputer atau server adalah *Packet Sniffing*, *Spoofing*, *Distributed Denial of Service* (DDoS), DNS *Poisoning*, *Trojan Horse*, SQL *Injection*, *Script kiddies*, LAND *Attack*, dan lain sebagainya (Irawan, 2022).

Berkaitan dengan perbuatan ini, klasifikasi perbuatan yang dilarang dalam UU ITE juga dijelaskan Pasal 27 hingga pasal 37, yang beberapa diantaranya dapat dikelompokkan ke dalam bentuk seperti, *unauthorized access to computer system and service, ilegal contents, data forgery, cyber espionage, cyber sabotage and extortion, offense against intellectual property,* dan *infrigments of privacy* (Sangga Buana & Rijal, 2021).

Secara umum, sebuah sistem yang aman akan mampu melindungi data yang ada didalamnya, namun keamanan sebuah sistem memungkin terkena serangan yang antara lain sebagai berikut (Paryati, 2008):

1. *Instrusion*

   Serangan ini terjadi pada sebuah sistem yang dilakukan untuk memiliki sebuah akses seperti

sebagaimana pengguna yang memiliki hak untuk mengakses sistem tersebut.

2. *Denial of Services*

   Serangan ini mengakibatkan pengguna yang sah tidak dapat mengakses sistem karena terjadi kemacetan pada sistem.

3. *Joyrider*

   Serangan ini dilakukan oleh pelaku yang ingin memperoleh kesenangan dengan cara menyerang suatu sistem untuk mendapatkan data yang dianggap menarik yang menyebabkan terjadinya kerusakan atau kehilangan data.

4. *Vandal*

   Serangan ini memiliki tujuan untuk merusak sebuah sistem, namun biasanya hanya dilakukan terhadap situs-situs yang besar, baik milik instansi, ataupun perorangan.

5. *Hijacking*

   Serangan ini menempatkan sebuah sistem monitoring atau memata-matai pengetikan ataupun aktifitas yang dilakukan pengguna pada *device*. Biasanya, serangan ini membutuh program khusus seperti *keylog* atau sejenisnya.

6. *Sniffing*

   Serangan ini memonitoring atau melakukan penangkapan terhadap paket data yang ditransmisikan dari computer client ke *web server* pada jaringan internet (saluran komunikasi).

7. *Spoofing*

   Serangan yang dilakukan dengan menampilkan halaman situs palsu untuk mendapatkan informasi

rahasia dari pengguna kepada pihak yang tidak memiliki hak.

8. *Website Defacting*

   Serangan yang dilakukan terhadap sebuah *website* dengan merubah isi halaman pada server yang bertujuan untuk membuat sebuah sarana yang seharusnya memberikan kemudahan menjadi tidak berfungsi secara baik.

9. *Virus*

   *Virus* adalah kode program yang dapat menyebabkan sebuah sistem bekerja di luar kehendak penggunanya, sehingga sebuah data atau *file* tertentu menjadi terinfeksi yang berakibat pada hilangnya file karena disembunyikan (*hide*), termodifikasi (*encrypt*) bahkan dapat terhapus (*delete*).

10. *Trojan Horse*

    Merupakan salah satu penyerangan dengan cara menyelinapkan sebuah program yang tidak dapat dilihat oleh *user* dalam suatu program yang dapat diunduh dan bersifat gratis, yang dapat menghapus data *user.*

11. *Worm*

    *Worm* adalah sebuah program yang dapat menduplikasikan diri melalui media computer yang berakibat pada kerusakan sistem serta memperlambat kerja sebuah sistem.

Adapun berbagai macam serangan terhadap sebuah sistem ini nantinya akan berguna untuk mengetahui apa saja

serangan yang dapat dilakukan, untuk kemudian dapat peneliti jadikan sebagai acuan pada penelitian ini.

### 2.3.5 Serangan-serangan pada *Web Server*

Serangan pada *web server* dapat berupa *SQL Injection, Cross Site Scripting (XSS), Denial of Service (DOS)* dan lain sebagainya yang berpotensi merugikan *server* maupun *client.*

Kerentanan ataupun serangan yang dapat dilakukan ataupun ditemukan pada masing-masing *layer* yang mengacu pada *Framerok* TCP/IP Model adalah sebagai berikut (MCMaster University, 2022):

***1. Application Layer***

Lapisan ini digunakan untuk melakukan komunikasi jaringan oleh sebagian besar program melalui data yang diteruskan dalam sebuah format khusus, kemudian dienkapsulasi ke dalam protokol lapisan transport. Kerentanan ataupun serangan yang dapat dilakukan pada *layer* ini adalah SQL *Injection* yaitu teknik eksploitasi yang terjadi pada lapisan basis data suatu aplikasi.

**2. *Transport Layer***

Lapisan ini bertanggung jawab untuk melakukan transfer pesan *end-to-end* yang independent dari jaringan yang mendasarinya, bersama dengan kontrol kesalahan, fragmentasi, dan kontrol aliran. Kerentanan ataupun serangan yang dapat dilakukan pada *layer* ini adalah *Port Scan Attack*, yaitu penyerangan untuk menemukan layanan atau port yang terbuka.

**3. *Network Layer***

Lapisan ini memecahkan masalah untuk mendapatkan paket di satu jaringan dengan protokol X.25 dan Protokol Host/IMP ARPANET. Kerentanan ataupun serangan yag dapat dilakukan pada lapisan ini adalah *Denial Of Service*.

**4. *Data Link Layer***

Lapisan ini memisahkan paket dari lapisan jaringan pada dua host yang berbeda. Kerentanan ataupun serangan yang dapat dilakukan pada lapisan ini adalah *Media Access Conrol* (MAC) *Address Spoofing*, yaitu serangan

untuk mencoba membuat *frame switch forward* target yang ditujukan untuk host jarak jauh ke penyerang *jaringan*.

***5. Physical Layer***

Lapisan ini bertanggung jawab untuk penyandian dan transmisi data melalui media komunikasi jaringan dalam bentuk bit. Kerentanan ataupun serangan yang dapat dilakukan pada serangan ini adalah serangan secara fisik seperti pengambilan atau pencurian kartu jaringan atau mencabut kabel tertentu.

Beberapa jenis serangan server seperti *SQL Injection*, *Cross Site Scripting (XSS), Denial of Service (DOS)* terjadi pada *Application Layer* dan *Network Layer*, tapi tidak menutup kemungkinan untuk dapat terjadi penyerangan pada *Layer* yang lain.

### 2.3.6 Jenis-jenis *Web Server*

*Web* Server adalah tulang belakang dari *world wide web* (www). *Web server* menunggu permintaan dari client yang menggunakan browser *seperti* untuk kemudian memproses permintaan itu dan memberikan hasil prosesnya berupa data yang diinginkan kembali ke *browser* (Hasbullah, 2018). *Web Server* adalah perangkat lunak yang memberikan layanan data-data pada *web client* atau *browser*. *Web server* pada dasarnya memiliki fungsi yang sama meskipun berbeda jenisnya, yaitu sebagai berikut (Cloudmatika, 2022).

1. *Nginx*, adalah *web server* dengan lisensi *open source* dengan kelebihan mampu menangani kebutuhan *web server* dengan trafik yang sangat tinggi.
2. *Apache HTTP Server, Web Server* yang didesain untuk sistem operasi UNIX dan dapat disebut sebagai competitor *Nginx*. *Apache* memiliki keunggulan dapat beroperasi dalam berbagai sistem operasi.
3. *Lighttpd*, adalah *Web Server* bersifat *open source* yang hanya bias berjalan pada sistem operasi LINUX dan UNIX atau turunan dari keduanya, dengan kelebihan mampu mengatur CPU *load* dengan lebih efisien.

4. *IIS (Internet Information Services)*, *Web Server* berbayar yang didukung oleh berbagai fitur dan komponen mulai dari TCP/IP, DNS, hingga *software* untuk membuat situs *web*. Selain itu, *IIS* menjadi satu-satunya *web server* yang mendukung *platform* .NET dari *Windows*.
5. *Sun Java System Web Server*, adalah *Web Server open source* yang cukup mudah dan didukung oleh tampilan visual dan *Graphical User Interface (GUI)* yang bersih. Namun, masih belum banyak yang menggunakannya.
6. *Litespeed*, adalah *Web Server* dengan performa mencapai enam kali lebih cepat dari *Apache*. Selain itu, juga terdapat fitur *Distributed Denial of Service (DdoS)*.

Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan menggunakan *web server* dengan jenis *Nginx* yang penulis ketahui melalui *Information Gathering* yang penulis lakukan berdasarkan pada Gambar 4.5. Adapaun kelebihan dan kekurangan dari *Nginx* adalah sebagai berikut (Jiwandono, 2021).

**Tabel 2. 1** Kelebihan dan Kekurangan Nginx

| Kelebihan | Kekurangan |
|---|---|
| Tangguh dalam menangani trafik yang tinggi | Update yang cukup lama disbanding *web server* lainnya |
| Skalabilitas Tinggi | *Fast* CGI yang tidak berfungsi sempurna |
| Bisa mengganti *Hardware Load Balancer* | Ditemukan masalah pada .htaccess, namun tergantung konfigurasi *web master*nya tersendiri |
| Mempunya *tool* multifungsi | Pemakai tidak sebanyak Apache IIS |
| Tersedia dokumentasi yang lengkap | |

Berdasarkan CXSecurity, kerentanan pada masing-masing *web server* diketahui sebagai berikut (CXSecurity, 2023).

**Tabel 2. 2** Kerentanan pada Web Server

| | |
|---|---|
| *Nginx* | Nginx 1.20.0 *Denial Of Service* |
| | Nginx 1.20.0 *DNS Resolver Off-By-One Heap Write* |
| *Apache* | *Apache Tomcat Privilege Escalation* |
| | *Apache Tomcat On Ubuntu Log Init Privilege Escalation* |
| | *Apache CouchDB Erlang Remote Code Execution* |
| *Lighttpd* | *Lighttpd 1.4.34 SQL Injection and Path Traversal* |
| | *Lighttpd Multiple Issues (Setuid unchecked; FAM read after free)* |
| IIS | *Polymail.io PPI Scanner/Insecure - IIS 7.5/Source Code Information Disc.* |
| | *IIS Group Admin Panel Bypass and SQL Injection Vulnerability* |
| *Sun Java System Web Server* | *Oracle Sun Java System Web Server – HTTP Response Splitting* |
| | *Glassfish Web Admin Interface (Sun Java System Application Server 9.1-01)* |
| *Litespeed* | *Openlitespeed 1.7.9 Notes Stored Cross-Site Scripting* |
| | *LiteSpeed Web Server Enterprise 5.4.11 Command Injection* |

### 2.3.7 *Website*

*Web* adalah sebuah situs atau portal. *Web* juga disebut sebagai kumpulan halaman *web* yang berhubungan antara satu dengan yang lainnya. Berdasarkan hal ini, dapat ditarik pemahaman bahwa *website* adalah sistus yang dapat diakses dan dilihat oleh para pengguna Internet (Abas, 2013).

Menurut Prasetiadi (2011), *web* adalah sekumpulan dokumen yang sangat banyak yang berada pada komputer server (*web server*). Melalui *web,* pengguna dapat mengakses berbagai informasi yang sedemikian rupa. Tidak hanya berbentuk teks, melainkan juga terdapa beberapa informasi seperti suara, gambar, video, dan animasi. Istilah mengenai *web,* sering kita lihat dalam *browser*.

*Website* juga disebut sebagai sejumlah halaman yang ditulis dengan kode tertentu HTML (*Hyper Text Markup Language*) dan memuat berbagai macam informasi yang saling berkaitan (Aini et al., 2019).

WWW (*World Wide Web*) adalah kelompok lokasi internet yang berkembang dan membentuk dokumen-dokumen *web,* atau halaman-halaman *web* untuk disajikan kepada pengguna Internet yang menjalankan *browser,* yaitu program yang diperlukan unutk menggunakan *web* (Snell, 1997).

Terdapat juga pendapat lain mengenai pengertian *website* menurut DzulfIqar (2017) yang mendefinisikan website sebagai sekumpulan layanan berisi informasi, iklan, ataupun program aplikasi untuk melakukan penelusuran informasi di internet.

*Website* tersimpan dalam *web server* yang mendukung kinerja dari *website* itu sendiri, yang bekerja untuk melayani permintaan pengguna berupa http dari *client* yang terhubung dalam sebuah jaringan dan memunculkan sebuah informasi berupa halaman *web* yang ditampilkan dalam *browser* (Monteiro et al., 2013). Berkaitan dengan pelayanan *server*, dibutuhkan aplikasi pada sebuah sistem komputer yang berfungsi untuk

memberikan pelayanan atas permintaan akses dari komputer pengguna. Terdapat beberapa aplikasi pelayanan *server* yang diantaranya, *Web Server*, FTP *Server*, DHCP *Server*, *Mail Server*, DNS *Server*, dan *Database Server* (Aziz & Tampati, 2015).

*Website* juga memiliki kualitas yang dikemukakan dalam beberapa dimensi seperti, kualitas sistem (*system quality*), kualitas informasi (*information quality*), dan kualitas layanan (*service quality*) yang akan menjadi perhatian bagi kebanyakan orang dalam menilai suatu kualitas (Ichsani, 2018).

*Website* berdasarkan sifatnya memiliki dua jenis, yaitu *website* statis dan *website* dinamis. *Website* statis adalah merupakan sebuah *website* dengan kondisi dimana konten didalamnya sangat jarang dirubah. Umumnya, Bahasa pemrograman yang digunakan adalah HTML dan belum menggunakan *database*. Sedangkan *website* dinamis adalah sebuah *website* yang memberikan konten atau isi yang sering berubah. Bahasa pemrograman yang digunakan antara lain, PHP, ASP, NET dan memanfaatkan *database* (Chandra et al., 2021).

Berdasarkan OWASP TOP 10 terdapat berbagai kerentanan pada *web* yang dapat ditemukan berkaitan dengan lemahnya keamanan yang diterapkan sebagai berikut (Owasp, 2021).

**Tabel 2. 3** Kerentanan pada Web berdasarkan OWASP TOP 10

| | | |
|---|---|---|
| 1 | *Broken Access Control* | Kerentanan ini menyebabkan terjadinya pengungkapan informasi yang tidak sah, modifikasi, atau penghancuran data. |
| 2 | *Cryptographic Failures* | Kerentanan ini menyebabkan kegagalan perlindungan data seperti kata sandi, informasi pribadi |

| | | |
|---|---|---|
| | | dan berbagai informasi penting lainnya. |
| 3 | *Injection* | Kerentanan terhadap serangan seperti SQL, NoSQL, dan lain sebagainya. |
| 4 | *Insecure Design* | Kerentanan ini menyebabkan kontrol keamanan tidak dapat bertahan atas serangan, karena kurangnya profil risiko bisnis pada sistem. |
| 5 | *Security Missconfiguration* | Tidak adanya penguatan keamanan yang sesuai, pengaturan keamanan pada kerangka kerja aplikasi tidak di *set* ke nilai *secure*; Tanpa konfigurasi keamanan yang terpadu, sistem dapat berada pada risiko yang lebih tinggi |
| 6 | *Vulnerable and Outdated Components* | Kerentanan yang berkaitan dengan versi komponen yang digunakan baik dari *client side* maupun *server* |
| 7 | *Identification and Authentication Failures* | Kerentanan yang dapat terjadi apabila penyerang memiliki akses kredensial, kata sandi yang lemah atau default, autentifikasi multifactor yang hilang atau |

| | | |
|---|---|---|
| | | tidak efektif, mengekspos pengidentifikasi sesi di URL, tidak membatalkan ID Sesi dengan benar dapat menyebabkan terjadinya serangan terkait autentikasi |
| 8 | *Software and Data Integrity Failures* | Kerentanan ini tidak dapat melindungi kita dari pelanggaran integritas, seperti ketergantungan aplikasi pada *plugin*, repositori, dan lain sebagainya. |
| 9 | *Security Logging and Monitoring Failures* | Kerentanan ini terjadi akibat kegagalan pendeteksian sehingga pelanggaran tidak dapat didetksi dan terjadi penyerangan |
| 10 | *Server-Side Request Forgery* | Kerentanan SSRF terjadi setiap kali *web* mengambil sumber jarak jauh tanpa melakukan validasi URL yang disediakan pengguna |

### 2.3.8 *Web Security*

*Web security* (Keamanan web) mengacu pada perlindungan jaringan dan sistem komputer dari kerusakan atau pencurian perangkat lunak, perangkat keras, ataupun data yang berarti termasuk keamanan untuk melindungi sistem komputer dari gangguan layanan yang dirancang (Fortinet, 2023). Erat kaitannya dengan *cyber security* disebabkan oleh

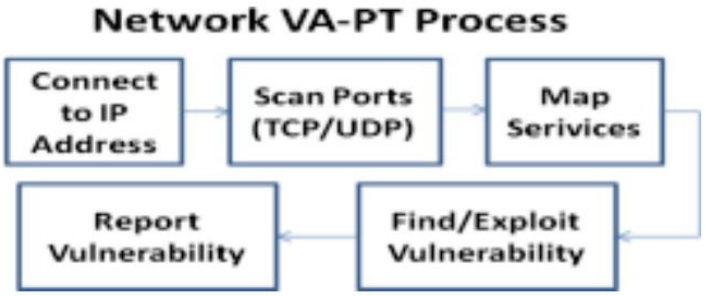
ruang lingkup yang merujuk pada interaksi antara orang, perangkat lunak, dan layanan yang terkoneksi internet (Budi et al., 2021), yang didalamnya terdapat beberapa jenis keamanan yang turut berkaitan dengan *web security* diantaranya, *cloud security*, *network security*, dan *application security* (Run System, 2022).

*Cloud Security* adalah sebuah layanan yang meliputi teknologi, kebijakan dan berbagai layanan lainnya yang berhubungan dengan *cloud security*. Beberapa cara diantaranya adalah menggunakan *firewall, two factor authentication*, hingga enkripsi data. Sedangkan *network security* sebagai salah satu dari jenis keamanan siber ini memiliki tujuan untuk melindungi berbagai data dan informasi penting serta jaringan lalu lintas data agar dapat terhindar dari pencurian data (Run System, 2022). Selain itu, *application security* adalah sebuah praktik penggunaan perangkat lunak, perangkat keras, dan berbagai prosedur lainnya untuk melindungi sistem dari ancamanan keamanan eksternal. *Application security* bekerja dengan tujuan akhir mencegah penyerang untuk mampu mengakses, mengubah, menghapus data atau informasi penting (Loshin, 2022).

Berdasarkan beberapa kaitan dengan keamanan lainnya yang dijabarkan diatas, terdapat beberapa teknologi yang dapat digunakan untuk memakmisalkan keamanan dari sebuah *web*, termasuk *Web Application Firewall* (WAF), pemindaia kerentanan, alat pembobol kata sandi, alat *fuzzing*, *black-box testing*, *white-box* testing yang dapat sangat membantu meningkatkan *web security* (Fortinet, 2023).

Pada Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, menggunakan WAF (*Web Application Firewall*) dengan jenis ‘Apache Generic’ yang penulis dapatkan melalui pengecekan pada Gambar 4.26 untuk melakukan pengamanan. Serta dengan menggunakan *Honeypot* sebagai *server* umpan yang dapat menjauhkan penyerang dari target utama ataupun sebuah hal yang penting untuk kemudian mampu untuk mengidentifikasi serangan lebih awal dan menyusun atau mempersiapkan respon yang sesuai.

### 2.3.9 *Vulnerability Assessment* dan *Penetration Testing*



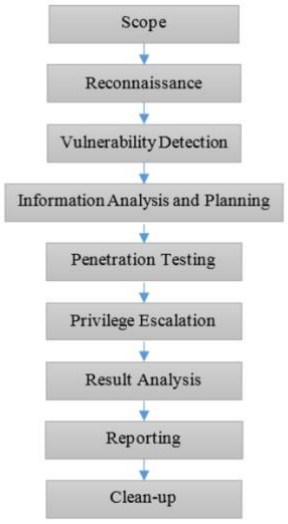

Gambar 2. 9 Proses VAPT Jaringan

*Vulnerability Assessment and Penetration Testing* adalah satu kesatuan bagian yang perlu ditempuh prosesnya satu demi satu. *Vulnerability Assessment* itu sendiri berarti tahapan pemindaian sistem atau perangkat lunak atau jaringan untuk mencari dan mengetahui kelemahan serta celah didalamnya. Celah yang ditemukan ini nantinya akan memberikan *backdoor* kepada penyerang untuk melakukan penyerangan terhadap korbannya (Goel & Mehtre, 2015). Kerentanan memiliki banyak jenis, namun beberapa diantaranya adalah:

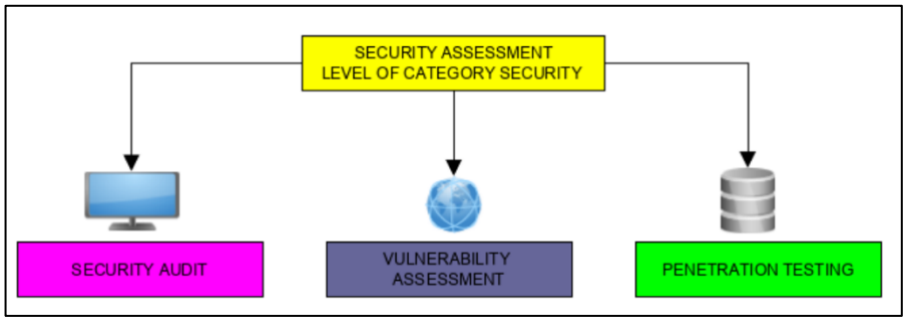
1. *Vulnerability of Boundary Condition*
2. *Vulnerabilities of Authentication*
3. *Vulnerability of Weakness in Configuration*
4. *Vulnerabilities of Exception Handling*

Penetration *Testing* adalah langkah lanjutan dari *Vulnerability Assessment*, dimana tahap ini dilakukan untuk mencoba mengeksploitasi sistem untuk mengetahui berbagai kemungkinan eksploitasi yang dapat dilakuka didalamnya. Dalam tahap ini, penulis memiliki otoritas untuk melakukan pengujian penetrasi dan secara maksimal mengeksploitasi sistem untuk mencari tahu kemungkinan eksploitasi terhadap sistem melalui berbagai celah.

*Vulnerability Assessment* dan *Penetration Testing* memiliki 9 langkah proses sebagai berikut (Goel & Mehtre, 2015).




Gambar 2. 10 Vulnerability Assessment dan Penetration Testing Life Cycle




Gambar 2. 11 Security Assessment Category Level

Berdasarkan gambar diatas, diketahui terdapat tiga level pada *security assessment* yaitu *security audit*, *vulnerability assessment*, dan *penetration testing*. Ketiganya memiliki tujuan yang sama untuk melakukan upaya keamanan pada sebuah sistem yang kita miliki (Zen et al., 2020). Pada penelitian ini, penulis menggabungkan *vulnerability assessment* dan *penetration testing* karena menggabungkan keduanya dapat memberikan perbaikan dan penjaminan keamanan secara lebih baik. Selain itu, 9 tahapan VAPT

yang dijelaskan pada gambar 2.10 memiliki langkah yang serupa dengan empat tahapan sederhana pada metode *Zero Entry Hacking* yang dijelaskan pada sub bab 2.11.1 dan sub bab 2.11.2, sehingga penelitian ini menggunakan metode *Zero Entry Hacking* sebagai satu kesatuan proses yang diterapkan pada *Vulnerability Assessment* dan *Penetration Testing*.

#### 2.3.9.1 *Vulnerability Assessment* (Penilaian Celah Kerentanan)

*Vulnerability Assessment* atau Penilaian Celah Kerentanan adalah serangkaian upaya yang dilakukan untuk memantau dan mengevaluasi berbagai kerentanan yang ada pada sebuah sistem (Moret, 2014). *Vulnerability Assessment* adalah kegiatan yang dilakukan untuk mengidentifikasi celah atau titik rentang yang dapat dimasuki oleh penyerang, untuk kemudian melalui celah tersebut penyerang dapat mengeksploitasi kerentanan yang ada (Secura, 2018). *Vulnerability Assessment* atau Penilaian Celah Kerentanan menurut Engebretson (2013) disebut sebagai serangkaian proses yang dilakukan untuk melakukan peninjauan *services* dan *system* terkait potensi celah kerentanan yang dimiliki.

Berdasarkan beberapa penjelasan diatas dapat disimpulkan bahwa *Vulnerability Assessment* atau Penilaian Celah Kerentanan adalah suatu rangkaian proses yang dilakukan untuk melakukan tinjauan terhadap sebuah sistem atas celah kerentanan yang mungkin ditemukan.

#### 2.3.9.2 *Penetration Testing*

*Penetration Testing* dapat diartikan sebagai kegiatan yang digunakan untuk memeriksa eksploitasi dan kerentanan pada sistem. Upaya ini membantu para pengembang untuk membangun sistem yang secara aman dalam hal melindungi data atau informasi yang ada. *Penetration Testing* sangat

penting dilakukan oleh berbagai pihak untuk melindungi data atau informasi penting dari pihak luar, serta penting untuk memantau tingkat kerentanan pada masalah keamanan (Stefinko et al., 2016).

*Penetration Testing* disebut juga sebagai *subclass* dari *ethical hacking* yang terdiri dari sekumpulan metode dan prosedur dengan tujuan untuk menguji atau melindungi sebuah keamanan organisasi (Arafat, 2020).

*Penetration Testing* adalah serangkaian kegiatan yang didalamnya terdapat simulasi serangan nyata untuk menilai risiko terkait potensi celah kerentanan yang dapat dimanfaatkan sebagai pelanggaran keamanan (Weidman, 2014).

Selain itu, menurut Wardaya (2019) *penetration testing* adalah serangkaian kegiatan yang didalamnya terdapat sebuah simulasi dan dilakukan oleh pihak yang telah mendapatkan izin untuk melakukan eksploitasi sistem.

Berdasarkan beberapa penjelasan tersebut, dapat dipahami bahwa *Penetration Testing* adalah serangkaian kegiatan yang dlakukan untuk mencari celah kerentanan terkait potensi pelanggaran keamanan dengan menggunakan simulai penyerangan secara nyata.

Berkaitan dengan pelaksanaan *penetration testing*, terdapat jenis *penetration testing internal* dan *external*. *Penetation Testing Internal* adalah pengujian oleh penguji yang memiliki akses ke aplikasi belakang *firewall* untuk mensimulasikan serangan. Sedangkan *Penetration Testing External* adalah Pengujian yang menargetkan asset perusahaan yang terlihat di internet seperti, *web*, *email*, serta nama domain (DNS) untuk mendapatkan akses dan data.

Penelitian ini termasuk ke dalam jenis *Penetration Testing External* dengan berfokus pada ruang lingkup *Network Penetration Testing. Network Penetration Testing* adalah metode pengujian keamanan pada sistem jaringan yang melibatkan identifikasi potensi kerentanan dan pengujian untuk memastikan kerentanan yang ditemukan (Coding Studio Team, 2021).

## 2.4 *Common Vulnerability Scoring System* (CVSS)

Penilaian kerentanan dapat dilakukan melalui beberapa metode seperti CVSS (*Common Vulnerability Scoring System*), CWE (*Common Weakness Enumeration*), CVE (*Common Vulnerabilities and Exposures*), OWASP (*Open Web Application Security Project*), dan ISO/IEC 27001 dengan kelebihan dan kekurangannya masing-masing yang dapat penulis sajikan dalam tabel berikut.

**Tabel 2. 4** Kelebihan dan Kekurangan Metode Penilaian Kerentanan

| Jenis Penilaian Kerentanan | Kelebihan | Kekurangan |
|---|---|---|
| CVSS (*Common Vulnerability Scoring System*) | - *Open Framework*<br>- Acuan Penanganan Kerentanan<br>- Skor Penilaian Sederhana<br>- Dapat menentukan prioritas berdasarkan parameter tingkat kerentanan | - Memerlukan *crosscheck* terhadap CVE ataupun CWE untuk memvalidasi hasil tingkat kerentanan |

| | | |
|---|---|---|
| CWE (*Common Weaknes Enumeration*) | - Bersifat database dan dapat dicari berdasrkan *keyword* | - Tidak dapat melakukan input sendiri berdasarkan *vector-vector* penyerangan |
| CVE (*Common Vulnerabilities and Exposures*) | - Bersifat database dan dapat dicari berdasrkan *keyword* | - Tidak dapat melakukan input sendiri berdasarkan *vector-vector* penyerangan |
| OWASP (*Open Web Application Security Project*) | - Memiliki Standar keamanan *website* sendiri (OWASP ASVS)<br>- OWASP Top 10 (*Checklist* Standar Keamanan Website) | - Ruang lingkup informasi yang terlalu luas, sehingga penentuan prioritas cukup sulit ditentukan |
| ISO/IEC 27001 | - Identifikasi dan pengatasan masalah yang proaktif<br>- Manajemen risiko, ketahanan dunia maya, dan keunggulan operasional | - Terdapat 113 kontrol keamanan informasi dan memerlukan waktuyang lama untuk memilih parameter keamanannya. |

### 2.4.1 Pengertian *Common Vulnerability Scoring System (CVSS)*

*Common Vulnerability Scoring System* (CVSS) adalah kerangka kerja terbuka untuk mengkomunikasikan karakteristik dan tingkat kerentanan dari perangkat lunak. CVSS ini terdari dari tiga kelompok metrik yaitu, *Base, Temporal,* and *Environmental* (FIRST, 2019).

*The National Vulnerability Database* (NVD) menyediakan skor CVSS secara spesifik untuk kerentanan yang diketahui public. *Federal Information Processing Standardsi* (FIPS) dengan 199 kategori keamanan skor NVD CVSS dapat digunakan oleh Badan federal untuk mendapatkan skor terkait dampak yang disesuaikan dengan lingkungan lembaga masing-masing (Mell et al., 2007).

Beberapa keuntungan yang didapatkan jika menerapakan CVSS sebagai pengukur tingkat kerentanan, yaitu (Mell et al., 2007):

1. *Standardized Vulnerability Scores*

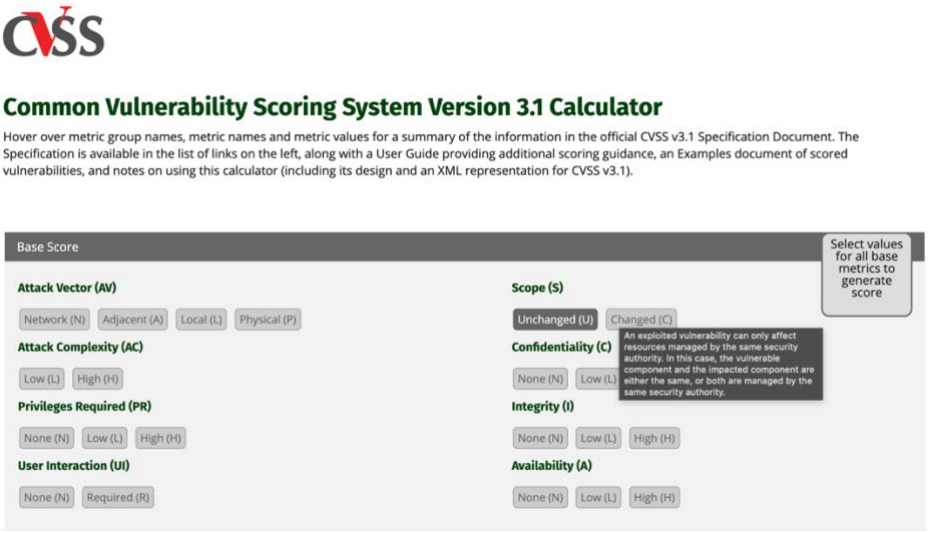
   Ketetapan ini dapat dikatakan serupa dengan perjanjian tingkat layanan (SLA) yang menyatakan seberapa cepat kerentanan tertentu harus divalidasi dan diperbaiki.

2. *Open Framework*

   Siapapun dapat melihat karakteristik individu yang digunakan untuk memperoleh skor.

*3.* *Prioritized Risk*

   Pada saat skor dihitung, kerentanan menjadi kontekstual. Hal ini dapat diartikan bahwa skor kerentanan mewakili risiko sebenarnya terhadap suatu organisasi. Pengguna dapat mengetahui betapa pentingnya suatu kerentanan dalam hubungannya dengan kerentanan yang lain.




Gambar 2. 12 Kalkulator CVSS V3.1

Kalkulator CVSS ini nantinya akan digunakan untuk mengukur sejauh mana tingkat kerentanan pada sebuah *website* untuk kemudian dapat dijadikan acuan untuk rekomendasi perbaikan dan lain sebagainya.

## 2.5 Jaringan Komputer

### 2.5.1 Pengertian Jaringan Komputer

Jaringan Komputer adalah jaringan telekomunikasi yang memungkinkan komputer satu dengan yang lainnya untuk saling berkomunikasi dengan bertukar data, jaringan komputer dibangun dengan kombinasi *hardware* dan *software*. Komputer yang saling terhubung ini harus mempunyai setidaknya 1 kartu jaringan masing-masing yang selanjutnya dihubungkan melalui kabel ataupun nirkabel yang bertindak sebagai media transmisi data. Selain itu juga terdapat *software* sistem operasi jaringan yang kemudian akan membentuk sebuah jaringan komputer sederhana (Astuti, 2018).

Dalam ilmu komputer, dua komputer atau lebih yang saling terhubung dan dapat menggunakan perangkat lain secara bersama, kemudian kelompok komputer akan didaftar ke dalam kelompok

atau grup yang sama dapat disebut sebagai *computer network* atau jaringan komputer (Victor Amrizal, M.Kom, 2015).

Jaringan Komputer juga dapat didefinisikan sebagai kumpulan perangkat berupa komputer, hub, *switch*, *router*, atau perangkat jaringan lainnya yang saling terhubung melalui media komunikasi tertentu. Perangkat yang saling berhubungan ini bekerja sama untuk mencapai tujuan yang sama (Adani, 2020).

Pengertian Jaringan Komputer juga disampaikan oleh Yudianto (2014), sebagai sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi.

### 2.5.2 Klasifikasi Jaringan Komputer

Tujuan dari jaringan komputer yang saling terhubung satu sama lain adalah untuk mencapai tujuan yang sama. Berdasarkan jangkauan geografis, jaringan komputer dapat dibedakan menjadi 3 bagian, yaitu diantaranya sebagai berikut (Yudianto, 2014):

#### 2.5.2.1 LAN (*Local Area Network*)

*Local Area Network* adalah jaringan komputer dengan jangkauan jaringan yang hanya mencakup wilayah kecil, seperti jaringan komputer di kampus, gedung, kantor, dalam rumah, sekolah ataupun ruang lingkup yang lebih kecil lagi. Secara umum, standar LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat *switch*, yang mempunyai kecepatan transfer data sebesar 10, 100, atau 1000 Mbit/s.

#### 2.5.2.2 WAN (Wide Area Network)

Wide Area Network adalah jaringan komputer dengan cakupan area yang besar. Jaringan ini digunakan untuk menghubungkan jaringan lokal yang satu dengan yang

lainnya. Hal ini dapat membuat pengguna atau komputer di lokasi yang berbeda dapat berkomunikasi satu sama lain. Sebagai contoh, jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat juga didefinisikan sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik.

#### 2.5.2.3 MAN (*Metropolitan Area Network*)

*Metropolitan Area Network* adalah suatu jaringan dengan transfer data berkecepatan tinggi yang menghubungkan berbagai lokasi dalam suatu kota. Umumnya, jaringan ini terdiri dari gabungan sejumlah LAN dengan jangkauan antara 10 hingga 50 km.

Berkaitan dengan hal ini, Informasi yang penulis dapatkan menjelaskan bahwa Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan menggunakan LAN untuk *local* di data center untuk kemudian akan terhubung dengan IP *Public*.

## 2.6 Protokol Jaringan

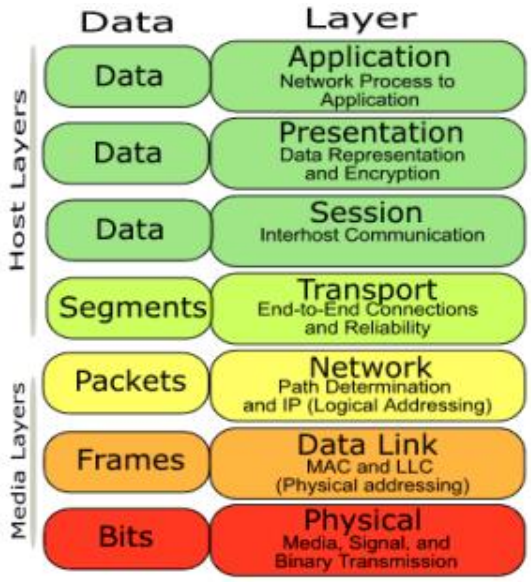
Protokol adalah seperangkat aturan yang digunakan agar sebuah jaringan dapat berkomunikasi dengan baik (Stallings, 2005). Dalam protokol, terdapat 3 buah fitur utama, yaitu:

1. Sintaks: Mempertimbangkan format blok data.
2. Semantik: Meliputi informasi control untuk koordinasi dan penanganan kesalahan.
3. Waktu: Termasuk kecepatan pencocokan dan urutan.

### 2.6.1 Model Referensi OSI

Model Referensi OSI (*Open System Interconnection*) adalah standar model referensi yang dikeluarkan oleh *Iternational Standart Organization* sebagai standarisasi protokol. Berdasarkan dokumen

rekomendasi X.200. standart OSI memiliki 7 layer dengan fungsi yang berbeda-beda,diantaranya (Saputro, 2014):




Gambar 2. 13 OSI Model

#### 2.6.1.1 *Layer* 7: *Application Layer*

Pada *layer* ini terjadi interaksi antarmuka *end user* dengan aplikasi yang bekerja melalui fungsionalitas jaringan, melakukan pengaturan bagaimana aplikasi bekerja menggunakan resource jaringan, untuk kemudian memberikan pesan Ketika terjadi kesalahan. Beberapa *service* dan protokol yang berada di layer ini misalnya HTTP, FTP, SMTP, dan lain sebagainya.

#### 2.6.1.2 *Layer* 6: *Presentation Layer*

*Layer* ini bekerja dengan mentranslasikan format data yang hendak di transmisikan oleh aplikasi melalui jaringan, ke dalam format yang bisa di transmisikan oleh jaringan. *Layer* ini juga akan meng-enkripsi atau men-deskripsi data.

#### 2.6.1.3 *Layer* 5: *Session Layer*

*Layer* ini akan memberikan pengertian terkait bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Di *layer* ini juga terdapat protokol *Name Recognition*, NFS & SMB.

#### 2.6.1.4 *Layer* 4: *Transport Layer*

Pada *layer* ini pemecahan data ke dalam paket-paket data serta pemberian nomor urut pada pake- paket data tersebut diberikan. Sehingga nantinya paket-paket data tersebut dapat disusun kembali saat sudah sampai pada sisi tujuan. Pada *layer* ini, protokol yang akan digunakan untuk mentransmisi data juga akan ditentukan, seperti halnya protokol TCP.

#### 2.6.1.5 *Layer* 3: *Network Layer*

*Network layer* akan membuat *header* untuk seluruh paket yang berisi informasi IP, baik pengirim data maupun IP tujuan data. Di kondisi tertentu, *network layer* akan melakukan routing melalui *internetworking* dengan menggunakan *router* dan *switch layer*-3.

#### 2.6.1.6 *Layer* 2: *Data-link Layer*

*Data-link layer* memiliki fungsi untuk menentukan bagaimana pengelompokkan bit-bit data menjadi sebuah format yang disebut *frame*. Pada *level* ini juga dilakukan pengoreksian kesalahan, *flow control*, pengalamatan *hardware* seperti halnya *Media Access Control Address* (MAC *Address*), dan penentuan terkait bagaimana perangkat-perangkat jaringan seperti *hub, bridge, repeater*, dan *switch layer* 2 beroperasi.

#### 2.6.1.7 *Layer* 1: *Physical Layer*

*Layer* ini berkerja dengan mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan, dan pengabelan. Selain itu, *Network Interface Card* (NIC) juga didefinisikan untuk mengetahui bagaimana interaksi dengan kabel atau radio dapat dilakukan.

### 2.6.2 Kerentanan Pada Masing-Masing *Layer* mengacu pada *Framework* TCP/IP *Protocol*

Kerentanan ataupun serangan yang dapat dilakukan ataupun ditemukan pada masing-masing *layer* yang mengacu pada *Framerok* TCP/IP Model adalah sebagai berikut (MCMaster University, 2022):

#### 2.6.2.1 *Application Layer*

Lapisan ini digunakan untuk melakukan komunikasi jaringan oleh sebagian besar program melalui data yang diteruskan dalam sebuah format khusus, kemudian dienkapsulasi ke dalam protokol lapisan transport. Kerentanan ataupun serangan yang dapat dilakukan pada *layer* ini adalah SQL *Injection*, XSS (*Cross Site Scripting*), *Missconfiguration directory permission*, *Sniffing Password*, *Spoofing, Spamming*, dan *Poisoning.*

#### 2.6.2.2 *Transport Layer*

Lapisan ini bertanggung jawab untuk melakukan transfer pesan *end-to-end* yang independent dari jaringan yang mendasarinya, bersama dengan kontrol kesalahan, fragmentasi, dan kontrol aliran. Kerentanan ataupun serangan yang dapat dilakukan pada *layer* ini adalah *Port Scan Attack*, Dos (*Denial of Service*), dan *Spoofing*.

#### 2.6.2.3 *Network Layer*

Lapisan ini memecahkan masalah untuk mendapatkan paket di satu jaringan dengan protokol X.25 dan Protokol Host/IMP ARPANET. Kerentanan ataupun serangan yag dapat dilakukan pada lapisan ini adalah *Smurf DoS* (*Denial Of Service), Teardrop Attack, Ping of Death*.

#### 2.6.2.4 *Data Link Layer*

Lapisan ini memisahkan paket dari lapisan jaringan pada dua host yang berbeda. Kerentanan ataupun serangan yang dapat dilakukan pada lapisan ini adalah *Media Access Conrol* (MAC) *Address Spoofing*, ARP *Poisoning*, *Passive Sniffing*.

#### 2.6.2.5 *Physical Layer*

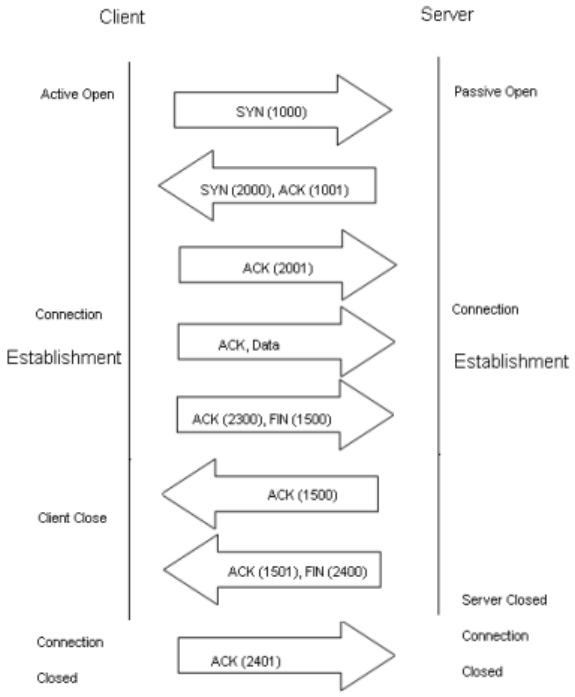
Lapisan ini bertanggung jawab untuk penyandian dan transmisi data melalui media komunikasi jaringan dalam bentuk bit. Kerentanan ataupun serangan yang dapat dilakukan pada serangan ini adalah serangan secara fisik seperti pengambilan atau pencurian kartu jaringan atau mencabut kabel tertentu.

### 2.6.3 *Transmission Control Protocol*/*Internet Protocol* (TCP/IP)

*Transmission Control Protocol*/*Internet Protocol* (TCP/IP) menyediakan fungsionalitas untuk interkoneksi sebuah sistem akhir di beberapa jaringan. Untuk tujuan ini, IP diimplementasikan di setiap sistem akhir dan di *router*, yang menyediakan koneksi antar jaringan (Stallings, 2005). TCP ini terletak pada *layer transport* dan menyediakan pelayanan yang dikenal sebagai *connection oriented*, *reliable*, *byte stear service*.

*Connection oriented* berarti sebelum melakukan pertukaran data, pengguna TCP harus melakukan pembentukan hubungan (*handshake*) terlebih dahulu. *Reliable* memberikan arti bahwa TCP

menerapkan proses deteksi kesalahan paket dan retransmisi. *Byte Stream Service* mengirimkan paket dan sampai ketujuan secara berurutan (Yunus & M. As'Ad, 2012).




Gambar 2. 14 Pembentukan dan Pemutusan Koneksi TCP

### 2.6.4 *UDP (User Datagram Protocol)*

Berbeda dengan TCP (*Transmission Control Protocol*), UDP bersifat *connectionless* dalam mentransmisi data dan tidak mengenal pengecekan terhadap error pengiriman data. Secara umum, protokol ini hanya mengandung IP dengan tambahan *header* singkat dan tidak melakukan sebuah proses kontrol alur data, kontrol kesalahan ataupun pengiriman ulang terhadap kesalahan sehingga hanya menyediakan *interface* ke protokol IP sehingga sangat berguna bagi situasi *client-server* (Mardiana & Sahputra, 2017).

Selain itu, Protokol ini juga tidak memerlukan *congestion control* atau kontrol kemacetan dalam koneksinya, yang dimaksudkan bahwa protokol ini dapat mengirimkan per *segment* tanpa dipengaruhi oleh kesibukan jaringan. Dengan sifat *unreliable*

atau dapat diartikan bahwa protokol ini akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan ACK (*Acknowledgement*). Adapun contoh protokol UDP yaitu, DNS, SNMP, TFTP, SunRPC port 111, dan lain sebagainya (Dwiyankuntoko, 2013).

### 2.6.5 Perbedaan TCP *(Transmission Control Protocol)* dan UDP *(User Datagram Protocol)*

Perbedaan TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*) akan dirangkum ke dalam tabel sebagai berikut (Klusaite, 2020).

**Tabel 2. 5** Perbedaan TCP dan UDP

| TCP | UDP |
|---|---|
| Menggunakan Koneksi | Tidak Memerlukan Koneksi |
| Berfungsi saat sebuah pesan dikirim dari satu komputer ke komputer lainnya saat sedang melintasi internet | Sebagai pengangkut pesan, dan dapat meneruskan paket yang dikirim ke pihak lain sehingga tidak berhenti di satu tempat |
| Diterapkan pada aplikasi dengan reabilitas tinggi dan waktu transfer data yang tidak terlalu cepat | Digunakan pada aplikasi yang memerlukan transfer data cepat |
| Sering digunakan untuk penjelajahan *web* seperti HTTP, HTTPS, Telnet, SMTP, FTP | DNS, RIP, DHCP, Layanan VOIP, TFTP, SNMP |
| TCP mengatur ulang paket data dan melakukan penomoran sesuai urutan | UDP tidak mengatur ulang paket |

| Lebih Lambat | Lebih Cepat |
|---|---|
| Penjaminan keutuhan data | Tidak menjamin |
| Memiliki ukuran *Header* sebesar 20 Byte | Memiliki ukuran *Header* sebesar 8 Byte |
| TCP memiliki beban yang berat | UDP terkenal ringan |
| Menggunakan 3 jabat tangan yaitu, *SYN, SYN-ACK* dan *ACK* | UDP tidak menggunakan jabat tangan sama sekali |

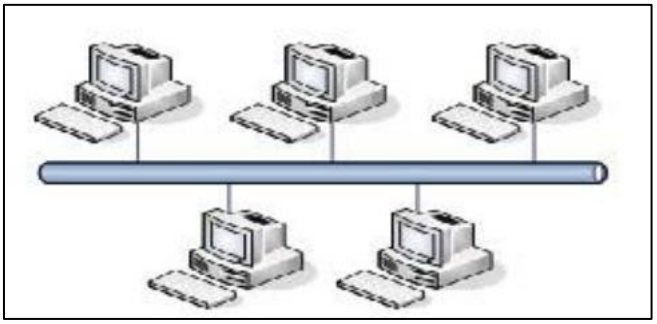
### 2.6.6 Topologi Jaringan

Topologi jaringan adalah sebuah cara untuk menghubungkan beberapa komputer untuk dapat menciptakan sebuah jaringan dengan berbagai susunan komputer yang kompleks (Anas et al., 2018). Selain itu, topologi jaringan juga berkenaan dengan penggambaran terkait bagaimana suatu jaringan didesain dengan aturan antara komponen untuk dapat berkomunikasi (Widodo et al., 2018). Topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) dan topologi logic (*logical topology*). Adapun jenis-jenis topologi jaringan yang dapat dijabarkan sebagai berikut (Yulianeu & Wahab, 2017).

1. Topologi Bus

   Topologi Bus atau *backbone,* memiliki sebuah kabel *coaxial* yang dibentangkan kemudian beberapa komputer dihubungkan pada kabel tersebut. Sederhananya, satu kabel media transmisi

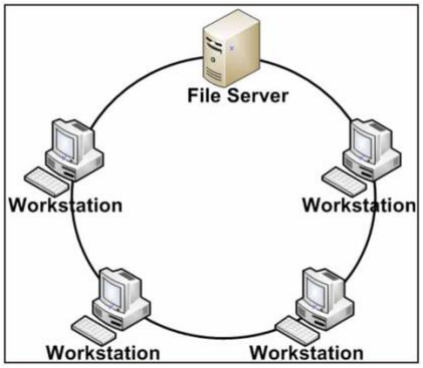
dibentang dari ujung ke ujung, kemudian kedua ujungnya ditutup dengan “terminator”.



Gambar 2. 15 Topologi Bus

2. Topologi Ring (Cincin)

   Topologi ring atau cincin adalah untaian media transmisi dari satu terminal ke terminal lainnya hingga membentuk suatu lingkaran satu arah. Terdapat tiga fungsi yang diperlukan dalam topologi ini, yaitu penyelipan data, penerimaan data, dan

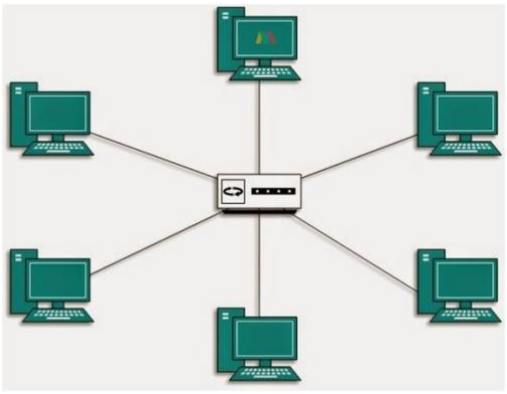



Gambar 2. 16 Topologi Ring

   pemindahan data.

3. Topologi Star (Bintang)

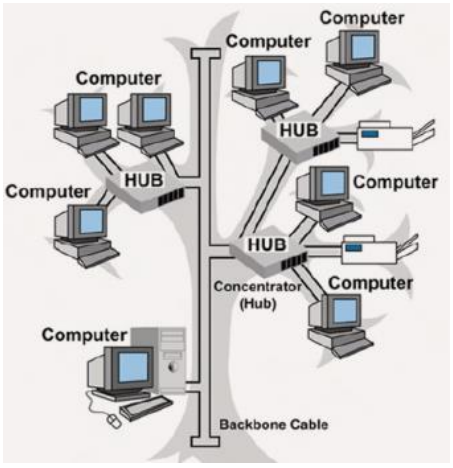
   Berbentuk seperti bintang, memiliki sebuah alat yang disebut *concentrator* atau bisa berupa *switch*, dimana semua komputer dalam jaringan dihubungkan ke *concentrator* ini. Pada topologi ini, sebuah terminal pusat bertindak sebagai pengatur dan pengendali seluruh komunikasi yang terjadi.



Gambar 2. 17 Topologi Star

4. Topologi Tree (Pohon)

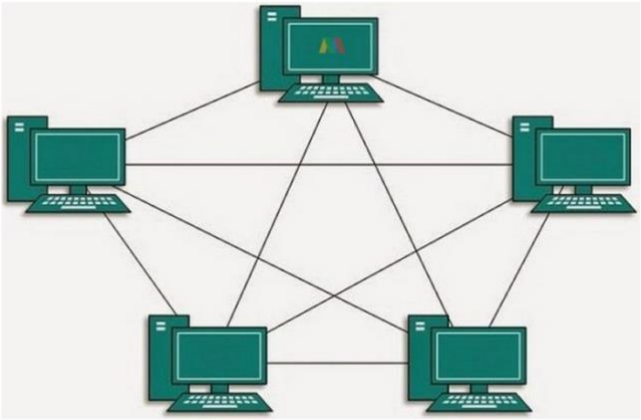
   Topologi ini adalah pengembangan atau generalisasi topologi bus dengan media transmisi satu kabel yang bercabang namun *loop* tidak tertutup. Topologi ini juga dimulai dari sebuah titik yang disebut '*headend'* yang kemudian beberapa kabel ditarik menjadi cabang, dan pada setiap cabang terhubung bebera terminal dalam bentuk bus atau dicabang lagi.




Gambar 2. 18 Topologi Tree

5. Topologi Mesh (Tak beraturan)

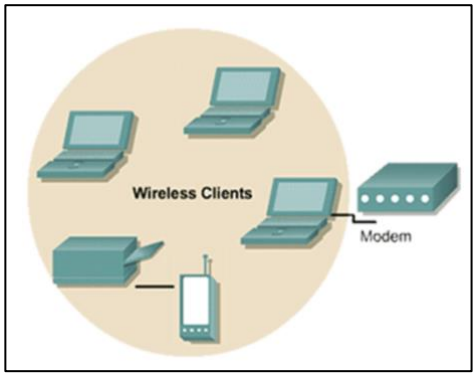
Topologi Mesh adalah topologi yang tidak memiliki aturan dalam koneksinya. Topologi ini muncul akibat tidak adanya perencanaan awal saat membangun suatu jaringan. Kegagalan komunikasi akan sulit dideteksi pada topologi ini.



Gambar 2. 19 Topologi Mesh

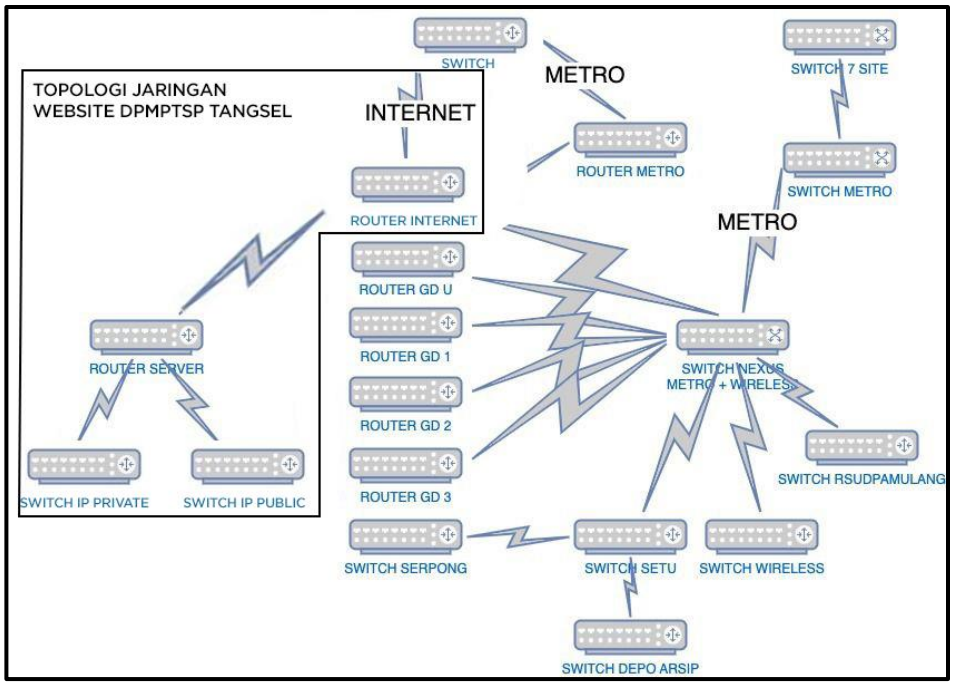
6. Topologi Wireless (Nirkabel)

   Topologi ini dikenal dengan berbagai nama, misalnya WLAN, WaveLAN, HotSpot, dan lain sebagainya. Topologi ini adalah nirkabel yang menjadi alternative jaringan kabel, untuk pengembangan LAN tradisional karena bisa menguras biaya pemasangan kabel dan mengurangi tugas.




Gambar 2. 20 Topologi Wireless

Dalam hal ini, terkait topologi jaringan pada Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan menggunakan jenis topologi *Tree* (Pohon) sebagai berikut.




Gambar 2. 21 Topologi Jaringan Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

Terkait sistem keamanan *Honeypot* dan WAF (*Web Application FIrewall*) yang diketahui berdasarkan hasil wawancara penulis dengan narasumber, *honeypot* berada di atas *Router Server* dan WAF (*Web Application Firewall*) terdapat pada masing-masing *server client*.

### 2.6.7 *Ports*

Dalam Ilmu Komputer, *port* logis adalah nomor yang ditetapkan untuk koneksi "logis". Secara lebih sederhana, dapat digambarkan sebagai titik akhir ke koneksi logis yang menggambarkan layanan di TCP/IP dan UDP. Nomor *port* ditetapkan ke layanan yang berguna untuk mengidentifikasi *port* mana yang harus dikirim lalu lintasnya.

*The Internet Assigned Number Authority* (IANA) menetapkan daftar *port* secara resmi dan mebaginya menjadi 3 bagian (The Cyber Security Man, 2018):

1. *Well-Known Ports* (0-1023)

   Nomor *port* dalam rentang *well-known ports* ditetapkan untuk protokol layanan yang umum digunakan dari *port* 0 hingga 1023. Selain itu, *port* ini juga dapat disebut sebagai "*port non-ephemeral*".

| PROTOCOL | PORT |
|---|---|
| FTP data port (Active Mode) | TCP 20 |
| FTP control port | TCP 21 |
| SSH | TCP 22 |
| SCP (uses SSH) | TCP 22 |
| SFTP (uses SSH) | TCP 22 |
| Telnet | TCP 23 |
| SMTP | TCP 25 |
| TACACS+ | TCP 49 |
| DNS name queries | UDP 53 |
| DNS zone transfers | TCP 53 |
| TFTP | UDP 69 |
| HTTP | TCP 80 |
| Kerberos | UDP/TCP 88 |
| POP3 | TCP 110 |
| SNMP | UDP 161 |
| SNMP trap | UDP 162 |
| NetBIOS (TCP rarely used) | TCP/UDP 137, 138, and TCP 139 |
| IMAP4 | TCP 143 |
| LDAP | TCP 389 |
| HTTPS | TCP 443 |
| SMTP with SSL/TLS | TCP 465 |
| IPsec (for VPN with IKE) | UDP 500 |
| LDAPv2 using SSL | TCP 636 |
| LDAPv3 using TLS | TCP 636 |
| IMAP using SSL/TLS | TCP 993 |
| POP using SSL/TLS | TCP 995 |
| L2TP | UDP 1701 |
| PPTP | TCP 1723 |
| RDP | TCP/UDP 3389 |
| Microsoft SQL Server | TCP 1433 |

Gambar 2. 22 *Well-Known Ports*

2. *Registered Ports* (1024-49,151)

   *Registered Ports* ditetapkan untuk mendukung kenyamanan perusahaan IT yang ingin mendaftarkan salah satu *port* logis untuk aplikasi berpemiliki seperti, Microsoft SQL, menggunakan TCP 1433.

3. *Dynamic*/*Private Ports* (49,152–65,535)

Rentang *port* ini juga disebut sebagai "*Port* Klien". Hal ini dikarenakan pada saat membuat koneksi dengan *web server*, *web browser* yang digunakan membuat koneksi ke *web server* melalui port 80 atau 443.

## 2.7 Internet

Internet merupakan kepanjangan dari *Interconnected Networking* yang mempunyai arti sebagai hubungan komputer dengan berbagai tipe yang membentuk sistem jaringan dalam cakupan seluruh dunia melalui jalur telekomunikasi. Internet juga merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda sistem operasinya maupun aplikasinya yang mana hubungan tersebut memanfaatkan kemajuan media komunikasi yang menggunakan standar protokol dalam berkomunikasi (Gani, 2014).

Menurut Bride (2003), internet adalah jaringan komputer global yang terbuka dan menghubungkan ribuan jaringan komputer melalui sambungan telepon umum ataupun pribadi. Selain itu, Bride juga menyampaikan bahwa internet merupakan hasil kerjasama antar jaringan komputer di seluruh dunia, baik yang berasal dari badan usaha komersial, dari lembaga pendidikan, maupun organisasi lainnya.

## 2.8 Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

Dinas Penanaman Modal dan Pelayanan Terpatu Satu Pintu (DPMPTSP) Kota Tangerang Selatan merupakan organisasi perangkat daerah yang dibentuk berdasarkan Peraturan Daerah Kota Tangerang Selatan Nomor 8 Tahun 2016 Tentang Pembentukan dan Susunan Perangkat daerah, dan peraturan Walikota Tangerang Selatan Nomor 61 tahun 2016, tentang Kedudukan, Struktur Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu. Adapun Visi dan Misi dari DPMPTSP Tangerang Selatan Sebagai berikut (Dpmptsp, 2023).

A. Visi

Terwujudnya Tangsel Unggul, Menuju Kota Lestari, Saling Terkoneksi, Efektif dan Efisien

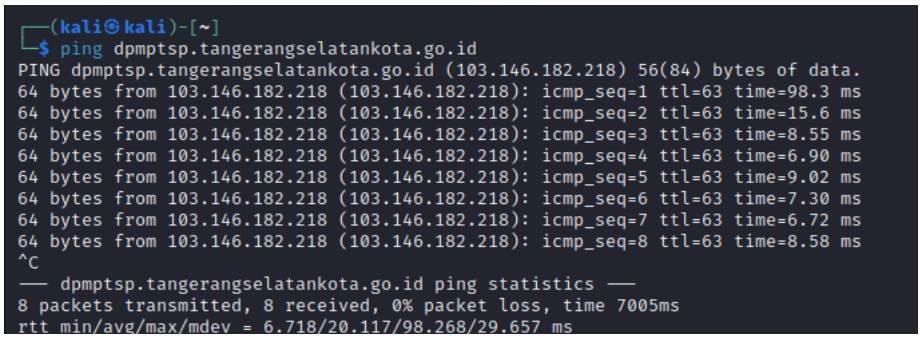
B. Misi

a. Pembangunan Sumber Daya Manusia (SDM) Yang Unggul
b. Pembangunan Infrastruktur Yang Saling Terkoneksi
c. Membangun Kota Yang Lestari
d. Meningkatkan Ekonomi Berbasis Nilai Tambah Tinggi Di Sektor Ekonomi Kreatif
e. Membangun Birokrasi Yang Efektif dan Efisien

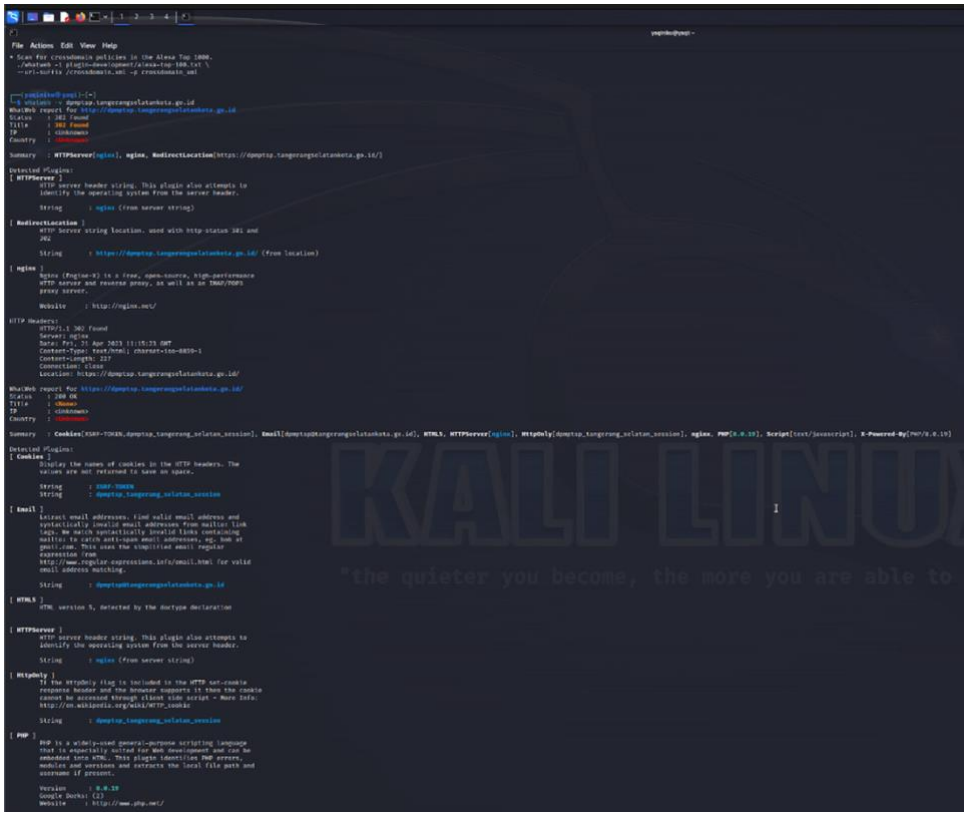
Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan memiliki *website* dengan alamat https://dpmptsp.tangerangselatankota.go.id/, yang menjadi sebuah layanan informasi yang sangat membantu memudahkan kebutuhan masyarakat yang berkepentingan.

Berdasarkan hasil *information gathering* menggunakan *tools whatweb* diketahui bahwa *website* ini menggunakan Nginx sebagai *web server* yang juga difungsikan sebagai *proxy server* untuk email (IMAP,POP3). Kemudian diketahui email yang digunakan adalah dpmptsp@tangerangselatankota.go.id, dan berdasarkan *doctype declaration website* ini menggunakan HTML 5 dan Bahasa PHP versi

8.0.19, dan *build in* menggunakan *framework* laravel dengan *IP Address* 103.146.182.218 yang dipaparkan pada gambar berikut.




Gambar 2. 24 Information Gathering dengan Ping



*Gambar 2. 23 Information Gathering* dengan *Whatweb*

Selain itu, berdasarkan hasil observasi dan wawancara yang dilakukan dengan Pak Ardan dan Pak Sru sebagai penanggung jawab *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan melalui media *online*

*Whatsapp*, diketahui bahwa Dinas Penanaman Modal telah melakukan pengamanan dengan menggunakan *Honeypot* dan *Web Application Firewall* (WAF) oleh Badan Siber dan Sandi Negara (BSSN), dan diketahui topologi jaringannya pada Gambar 2.20.

## 2.9 *Hacker*

*Hacker* adalah seseorang yang menggunakan sebuah komputer, jaringan, dan kemampuna lainnya untuk mengatasi suatu masalah teknis. Umumnya, kemampuan ini dimanfaatkan oleh sebagian dari mereka untuk melakukan suatu hal yang buruk. Berdasarkan perilakunya ataupun tujuan dari tindakannya, terdapat jenis *hacker* sebagai berikut (Cyber Academy Indonesia, 2022).

### 2.9.1 *Black Hat*

*Black Hat* ini dapat juga disebut dengan *Unethical Hacker* atau sederhananya adalah mereka yang melakukan peretasan pada sistem dengan tujuan yang buruk. Beberapa hal yang umumnya dilakukan adalah melakukan pencurian data atau informasi penting, pemerasan, modifikasi, dan berbagai tindakan illegal lainnya.

### 2.9.2 *White Hat*

*White Hat* adalah kebalikan dari *Black Hat* yang memiliki sebutan lain sebagai *Ethical Hacker*. Peretasan yang dilakukan oleh mereka bertujuan baik dan mendapatkan persetujuan dari pemilik sistem atau mereka yang memiliki hak. Tujuan dari *Ethical Hacker* ini adalah untuk mencari kemungkinan celah pada sebuah sistem untuk kemudian memberi tahu pemiliknya agar melakukan perbaikan.

### 2.9.3 *Grey Hat*

*Grey Hat* merupakan gabungan dari dua jenis *hacker* diatas, peretasan yang dilakukan tidak memiliki izin untuk melakukan

pengujian keamanan, namun mereka juga tidak akan mencuri data ataupun merusak sistem. Umumnya, saat menemukan celah *hacker Grey Hat* akan memberitahu pemilik sistem, namun sebelumnya mereka telah melihat informasi tanpa izin melalui celah yang telah mereka retas.

Dalam penelitian ini, penulis berperan sebagai *hacker* dengan jenis *White Hat* dengan alasan bahwa pengujian yang dilakukan telah mendapatkan izin resmi dari pihak Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, berdasarkan hasil surat permohonan yang telah penulis ajukan sebelumnya.

## 2.10 Pengujian Aplikasi

### 2.10.1 Teknik Pengujian *Software*

Pada pengujian *software* terdapat tiga macam pendekatan yang digunakan yang dapat digunakan sesuai kebutuhan, sebagai berikut:

1. *Black-box testing*

   *Black-box testing* menurut Cole (2005), disebut sebagai suatu rangkai uji yang dilakukan pada antarmuka *software* dan dilakukan pengujian beberapa aspek fundamental dari sebuah sistem dengan sedikit hal untuk struktur dari suatu *software*.

2. *White-box testing*

   Cole (2005), menjelaskan *white-box testing* sebagai serangkaian pengujian yang sifatnya mendasari pengujian secara ketat dari tahapan-tahapan yang terperinci. Berdasarkan hal tersebut, dapat diketahui bahwa metode ini adalah pengujian yang dilakukan secara mendalam dan menyeluruh sehingga sistem yang tersaji dapat berjalan dengna sempurna.

3. *Grey-box testing*

*Grey-box testing* adalah Teknik uji aplikasi dengan pengetahuan yang terbatas tentang kerja internal aplikasi serta memiliki pengetahuan tentang aspek fundamental sistem. Dalam metode ini, kode dari dua model dipelajari dan digunakan untuk desain kasus uji dan tes sebenarnya pada antarmuka yang terbuka (Khan & Khan, 2012).

Teknik pengujian *software* yang digunakan pada penelitian ini adalah *black-box testing*. Hal ini dikarenakan penelitian ini tidak memiliki akses ke struktur internal, melainkan peneliti hanya berinteraksi dengan sistem melalui *input*nya dan mengamati *output* atau perilaku untuk mengevaluasi fungsi.

## 2.11 Pengujian dan Analisis

Sebagai satu kesatuan langkah dalam mengupayakan keamanan dari celah kerentanan yang ditemukan, *Vulnerability Assessment and Penetration Testing* (VAPT) memiliki keterkaitan satu sama lain. Dimulai dari proses pemindaian kerentanan, kemudian celah kerentanan yang ada akan di eksploitasi untuk mengetahui berbagai kemungkinan eksploitasi dalam sebuah sistem (Goel & Mehtre, 2015).

Pada *Penetration Testing*, terdapat beberapa metode yang dapat digunakan seperti OSSTM (*Open Source Security Testing Methodology Manual*), OWASP (*Open Web Application Security Project*), NIST (*National Institute of Standards and Technology*), PTES (*Penetration Testing Methodologies and Standards*), ISSAF (*Information System Security Assessment Framework*), ZEH (*Zero Entry Hacking*) (Germanotta, 2021).

**Tabel 2. 6** Kelebihan dan Kekurangan Metode *Penetration Testing*

| Metode | Kelebihan | Kekurangan |
|---|---|---|
| OSSTM (*Open Source Security* | - *Open Source* | - Kompleks dan membutuhkan |

| | | |
|---|---|---|
| *Testing Methodology Manual*) | - Mendukung tim pengembangan jaringan<br>- Memiliki 6 Tahapan | pemahaman yang lebih dalam tentang keamanan sistem<br>- Tergantung pengalamanan penguji atau pentester |
| OWASP (*Open Web Application Security Project*) | - Memiliki Standar keamanan *website* sendiri (OWASP ASVS)<br>OWASP Top 10 (*Checklist* Standar Keamanan Website) | Ruang lingkup informasi yang terlalu luas, sehingga penentuan prioritas cukup sulit ditentukan |
| NIST (*National Institute of Standards and Technology*) | - Memiliki panduan yang disediakan di NIST SP 800-53<br>- Memiliki 3 kelas kontrol keamanan<br>- Terdiri dari 6 fase pengukuran keamanan | - Terdiri dari 19 bidang pengukuran<br>- Ruang lingkup dan sumber daya yang besar |
| PTES (*Penetration Testing Methodologies and Standards*) | - Memiliki langkah uji penetrasi, komunikasi awal, pengumpulan informasi, dan | - Melibatkan keahlian dan penilaian dari seorang pentester<br>- Melalui banyak langkah |

| | | |
|---|---|---|
| | pemodelan ancaman<br>- Memiliki tujuh fase untuk menjamin uji penetrasi | |
| ISSAF (*Information System Security Assessment Framework*) | - Terstruktur dan khusus untuk pengujian penetration testing<br>- Kerangka kerja yang komprehensif<br>- Terperinci dengan Sembilan tahapan | - Sangat kompleks<br>- Keterbatasan pembaruan |
| WAPT (*Web Appliaction Penetration Testing*) | - Memiliki 5 tahapan pengujian<br>- Lebih sederhana dibandingkan beberapa metode lainnya | - Memerlukan sumber daya yang cukup banyak<br>- Memakan waktu yang lebih lama<br>- Dapat mengganggu operasional *website* |
| BSIMM (*Building Security In Maturity Model*) | - Kerangka kerja yang terstruktur<br>- Memiliki 112 kegiatan BSIMM dalam 4 domain | - Sangat kompleks untuk pemula<br>- Kurang fleksibel |

| | | |
|---|---|---|
| ZEH (*Zero Entry Hacking*) | - Memiliki 4 Tahapan sederhana<br>- Lebih mudah<br>- Tetap mampu memberikan hasil pengujian secara baik | - Tidak termasuk ke dalam metode umum yang diketahui oleh banyak orang |

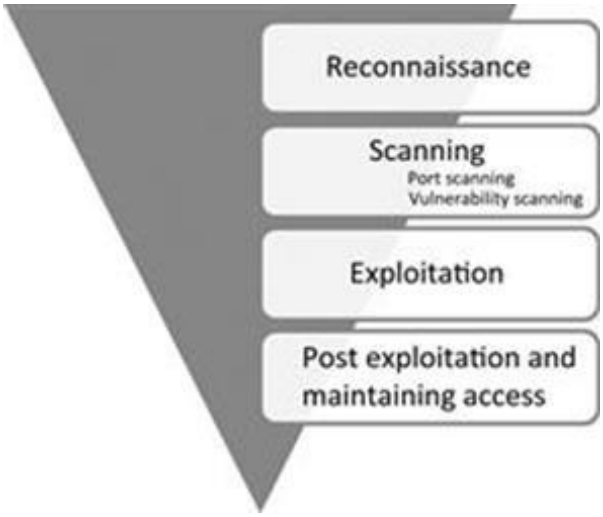
Berdasarkan Tabel 2.5 diatas, penulis menggunakan metode *Zero Entry Hacking* (ZEH) digunakan sebagai metode dalam pengujian penetrasi melalui empat tahapan yaitu, Pengintai Sistem (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi Celah Keamanan (*Exploitation*), dan PKasca Eksploitasi (*Post Exploitation*), karena memiliki empat tahapan sederhana yang sangat cocok untuk pemula namun tetap dapat memberikan hasil yang baik dalam pengujian kerentanan yang dapat diketahui berdasarkan beberapa penelitian sebelumnya. Selain itu, kompleksitas, waktu serta sumber daya yang dibutuhkan masih dapat dipertimbangkan.

### 2.11.1 *Zero Entry Hacking* (ZEH)

Pada penelitian ini, metodeologi yang digunakan dalam pengujian dan analisisnya ialah *Zero Entry Hacking* (ZEH). Metode ini merupakan metode yang dapat digunakan untuk melakukan tahap *Penetration Testing*. *Zero Entry Hacking* merupakan metodologi dengan 4 tahapan sederhana, sehingga metode ini disebut sebagai salah satu metode yang cocok digunakan oleh pemula (P. Engebretson, 2013).

### 2.11.2 Tahapan *Zero Entry Hacking* (ZEH)

Pada *Zero Entry Hacking* (ZEH) terdapat 4 tahapan yang harus dilalui dalam pengujian sistem. Tahapan-tahapan dalam metode ini menurut Engebretson (2013) yaitu, Pengintai Sistem (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi Celah Keamanan (*Exploitation*), dan Pasca Eksploitasi (*Post Exploitation*) yang ditampilkan pada gambar berikut.




Gambar 2. 25 Tahapan *Zero Entry Hacking* (ZEH)

Langkah-langkah pada Gambar 2.14 dapat dijelaskan sebagai berikut (Sahtyawan, 2019):

1. Pengintaian Sistem (*Reconnaisance*)

   *Reconnaisance* adalah langkah pertama yang dilakukan dengan merancang dan mencari informasi sebanyak mungkin dari sebuah target sebelum melakukan serangan yang dapat dilakukan dengan menggunakan beberapa *tools* seperti, shodan.io, perintah *ping*, *whois*, dnsmap, *theHarvester*, *whatweb*, dan lain sebagainya.

2. Pemindaian (*Scanning*)

   *Scanning* adalah sebuah tahapan dimana seorang penyerang menggunakan berbagai macam *tools* untuk mencari celah yang

akan digunakan sebagai target serangan seperti, Nessus, Nmap, Uniscan, Acunetix, dan lain sebagainya.

3. Eksploitasi Celah Keamanan (*Exploitation*)
   Pada tahap ini, celah kerentanan yang telah ditemukan akan di uji untuk memperoleh akses pada sebuah sistem tersebut dengan *tools* seperti, OWASP TOP 10, OWASP ZAP, Burp Suite, Nmap, dan lain sebagainya.
4. Pasca Eksploitasi (*Post Exploitation*)
   Pada tahap ini, akan dilakukan upaya untuk mempertahankan akses yang didapatkan, kemudian akan menambal lubang keamanan pada sistem dari ancaman penyusup yang dapat merubah data dan informasi yang ada, serta melakukan penghapusan jejak agar tidak diketahui lokasinya dengan tools *weevely*, dan *Microsoft word*.

## 2.12 Penelitian Eksperimen

Penelitian eksperimental dapat disebut sebagai salah satu pendekatan utama dalam penelitian Bahasa kedua, dan linguis terapan. Secara sederhana, penelitian ini dilakukan untuk mengetahui akibat dari perlakuan yang diberikan terhadap suatu hal yang sedang di teliti atau mencari pengaruh dari *treatment* tertentu. Beberapa hal yang menjadikan penelitian eksperimen berbeda adalah dengan adanya manipulasi variabel, control, penugasan *random*, dan perlakuan (*treatment*) (Asrin, 2022).

Variabel dalam penelitian eksperimen adalah segala sesuatu yang berakitan dengan berbagai kondisi, keadanaan, faktor, perlakuan, atau bentuk tindakamn yang diperkirakan dapat mempengaruhi hasil eksperimen. Berdasarkan beberapa penjelasan tersebut, dapat dipahami bahwa penelitian eksperimen adalah kegiatan penelitian yang dilakukan untuk mengetahui bagaimana pengaruh dari suatu tindakan terhadap sebuah subjek ataupun objek yang diteliti (Hidayat, 2021). Penelitian eksperimen memiliki beberapa jenis atau bentuk desain eksperimen yang meliputi, *Pre-*

*Experimental Design*, *True Experimental Design*, *Quasi-Experimental Design*, dan *Factorial Design* dengan ketentuan dan kondisi yang berbeda (Ratminingsih, 2010).

Berkitan dengan *design* metode penelitian, penulis menggunakan jenis *Pre-Experimental Design*. Desain metode penelitian ini memiliki tiga bentuk yaitu, *One-Shot Case Study*, *One-Group Pretest-Posttest Design*, dan *Intact-Group Comparisson*. Pada penelitian ini, penulis menggunakan jenis *Pre-Experimental* dengan bentuk desain *One Shot Case Study*, karena dalam penelitian ini hanya terdapat satu kelompok yang diberikan *treatment* atau perlakukan serta tidak ada kelompok pembanding, sehingga kelompok yang diberikan *treatment* atau perlakukan tersebut langsung diukur untuk dapat diketahui hasilnya (Hidayat, 2021). Untuk tahapan pada penelitian eksperimen ini, melalui 3 tiga tahapan utama yaitu (Thabroni, 2022).

1. Tahap Persiapan

   Perancangan eksperimen meliputi bentuk penelitian eksperimen dan desain yang akan digunakan, studi pustaka, dan lain sebagainya.
2. Pelaksanaan Penelitian

   Pada tahap ini, penelitian akan berlangsung dengan menggunakan metode pengujian *Zero Entry Hacking* dalam melakukan *penetration testing*.
3. Pengolahan dan Analisis data

   Hasil dari eksperimen akan diinterpretasikan melalui tabel kerentanan yang sebelumnya telah diukur menggunakan *Common Vulnerability Scoring System* (CVSS)

## 2.13 *Tools*/Teknologi yang Digunakan Untuk *Penetration Testing*

### 2.13.1 *Who Is*

*Who Is* adalah sebuah aplikasi berbasis website yang menawarkan fitur untuk mencari alamat IP di ribuan domain tingkat atas (TLD)

dan domain tingkat kedua (SLD), yang memberikan informasi berharga seperti pencatat domain, status, tanggal kadaluarsa, dan nama server DNS (Who.is, 2022). *Who Is* bekerja secara sederhana

Gambar 2. 26 Cara Menggunakan Whois

dengan menggunakan data yang tercatat saat pertama kali seseorang atau sebuah instansi membeli domain. Data ini nantinya akan disimpain oleh ICANN (*Internet Corporation for Assigned Names and Numbers*) di database mereka untuk kepentingan hak dan penggunaan nama domain. Ada beberapa cara yang dapat dilakukan untuk menggunakan *whois*, beberapa diantaranya, menggunakan *website tools whois lookup* melalui Whois.com, menggunakan *command line* di laptop dengan mengetikkan whois -v diikuti nama domain pada OS Windows, dan pada OS Mac dapat menggunakan Linux's *Lookup command* dengan membuka whois query di Mac dan mengetikkan whois diikuti nama domain (Kaurvaki, 2023). Pada penelitian ini, *tool whois* akan digunakan pada tahap *reconnaisance* yang dapat dilihat pada pembahasan sub bab 4.2.1.1.

### 2.13.2 *The Harvester*

*The Harvester* adalah alat yang dikembangan dengan python yang dapat digunakan untuk mengumpulkan informasi seperti *email*,

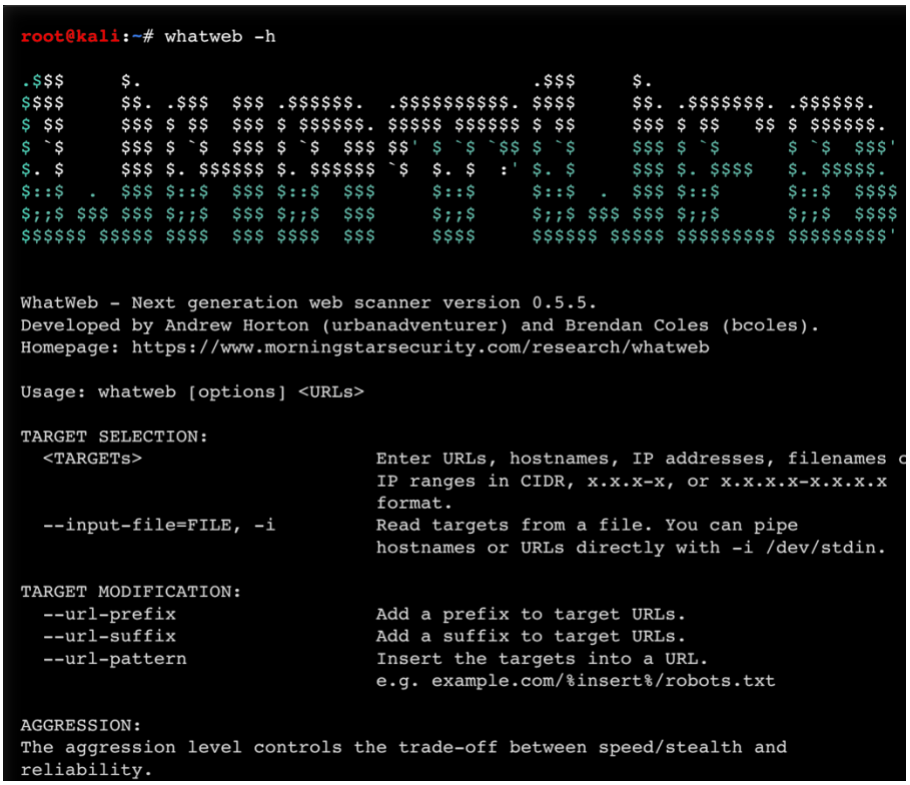
*subdomain*, *host*, nama karyawan, *port* yang terbuka, dan lain sebagainya. Alat ini dapat sangat berguna bagi pihak-pihak yang perlu mengetahui apa yang dapat dilihat oleh penyerang tentang sebuah sistem atau organisasi (Cybervie.com, 2022). Untuk mekanismenya pada Kali Linux, cukup unduh dan ekstrak file terkait the harvester kemudiamn berikan izin eksekusi dan jalankan ./theharvester. Kemudian, untuk mendapatkan semua informasi tentang situs *web* dapat menjalankan perintah 'theHarvester -d diikuti nama domain -l 300 -b all' (Paket Internet, 2020). *The Harvester* akan diterapkan penggunaannya pada tahap *reconnaisance* pada sub bab 4.2.1.3

Gambar 2. 27 Cara Menggunakan theHarvester

### 2.13.3 *What Web*

*What Web* digunakan untuk mengidentifikasi *website*, termasuk sistem manajemen konten, *blogging platforms*, *javascript*, *web servers*, dan perangkat yang disematkan. *What Web* menampilkan informasi lain seperti alamat *email*, nomor versi, ID akun, modul kerangka kerja *web*, kesalahan SQL, dan lain sebagainya. *Whatweb* memiliki ukuran instalasi sebesar 18.59 MB, dan untuk instalasi dapat menjalankan perintah 'sudo apt install whatweb'. Cara

menggunakan *whatweb* terbilang sederhana dengan menjalankan perintah ‘whatweb –help’ untuk melihat perintah dan opsi apa saja yang dapat digunakan (kali.org, 2022). *What web* akan digunakan dengan menuliskan perintah ‘*whatweb -v* alamat *-a 3*’ yang dapat dilihat pada sub bab 4.2.1.2.




Gambar 2. 28 Cara Menggunakan WhatWeb

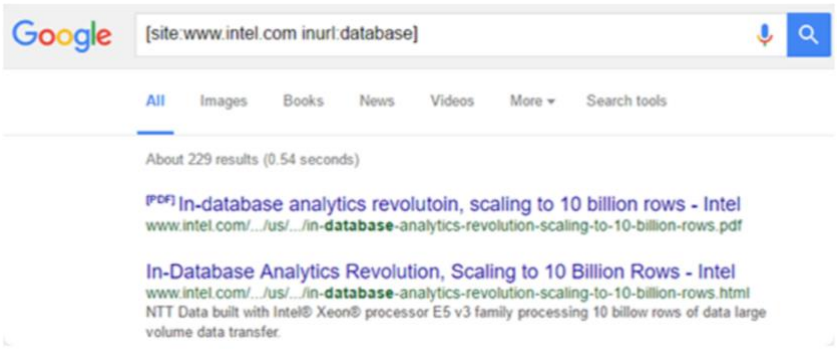
### 2.13.4 *CXSecurity*

*CXSecurity* adalah sekumpulan besar informasi mengenai keamanan komunikasi data yang bertujuan untuk memberi informasi tentang keamanan siber yang dikelola oleh satu orang *independent. Database* ini nantinya yang akan digunakan sebagai panduan untuk melakukan identifikasi terkait objek yang akan di uji (CXSecurity, 2023). Pengaplikasian *CXSecurity* pada tahap *reconnaisance* dapat dilihat pada sub bab 4.2.1.4.

Gambar 2. 29 Cara Mengakses CXSecurity

### 2.13.5 *Google Hacking Database* + *Google Dorking*

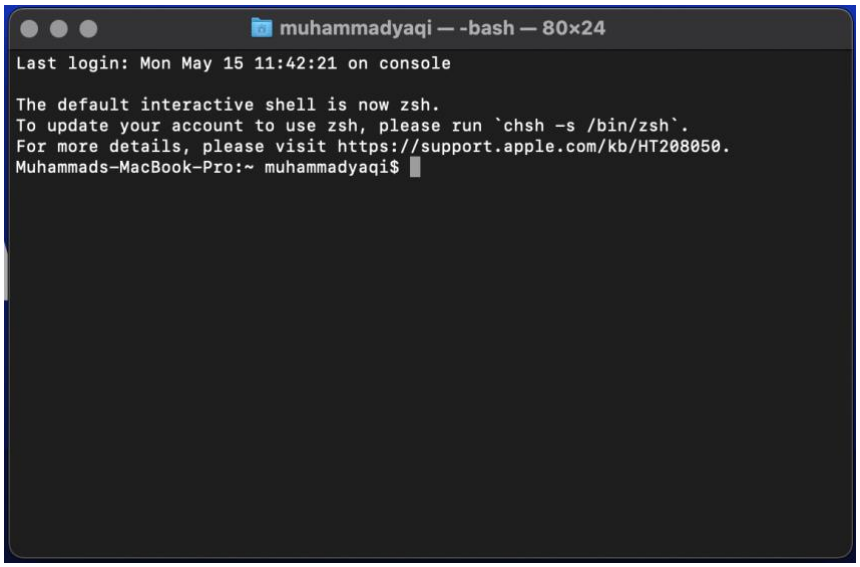
*Google* memperkenalkan fungsi kuat dari "*Directives*" dengan tujuan untuk membuat pencarian yang lebih kuat dan mengarah pada target perihal mengumpulkan informasi dan *file* dari *website* tertentu (P. H. Engebretson et al., 2008). *Google Dork* juga dapat disebut sebagai *Google Hack*ing, yang menggunakan *search string Advance Operators* untuk dapat menemukan sebuah informasi yang tidak mudah terlihat oleh publik yang kemudian akan digunakan untuk menemukan kerentanan pada sebuah situs *web* (Parmar, 2019). Pada sub bab 4.2.1.5, GHDB akan digunakan untuk mencari kerentanan dengan contoh penggunaan seperti gambar 2.29.




Gambar 2. 30 Contoh Penggunaan Google Hacking Database

### 2.13.6 Terminal

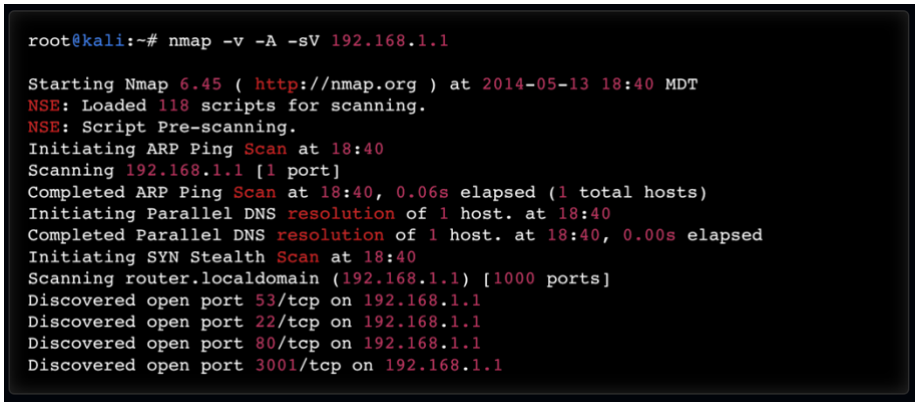
Terminal sering disebut *command prompt* atau *shell* yang digunakan sebagai peramban berkas untuk melayari berkas yang dimiliki dan membatalkan perubahan yang telah dibuat melalui penerapan perintah yang sudah ditentukan (Ubuntu, n.d.).




Gambar 2. 31 Terminal

### 2.13.7 Nmap

*Nmap* adalah singkatan dari *Network Mapper* yang berarti sebuah *tool open source* untuk melakukan eksplorasi dan audit keamanan jaringan. *Nmap* menggunakan paket *IP raw* untuk mendeteksi *host* yang terhubung dengan jaringan yang dilengkapi dengan layanan, sistem operasi, jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya (Bayu Rendro & Nugroho Aji, 2020). Nmap tersedia di *repository default* Ubuntu dan Debian dengan perintah instalasi sebagai berikut '$ sudo apt update', '$ sudo apt install nmap'. Untuk *scanning port* menggunakan Nmap, cara paling mudah yang dapat digunakan adalah melalui perintah '$ nmap scanme. diikuti nama domain' (Hamim, 2021). Penggunaan Nmap pada penelitian ini dapat dilihat pada sub bab 4.2.2.2.

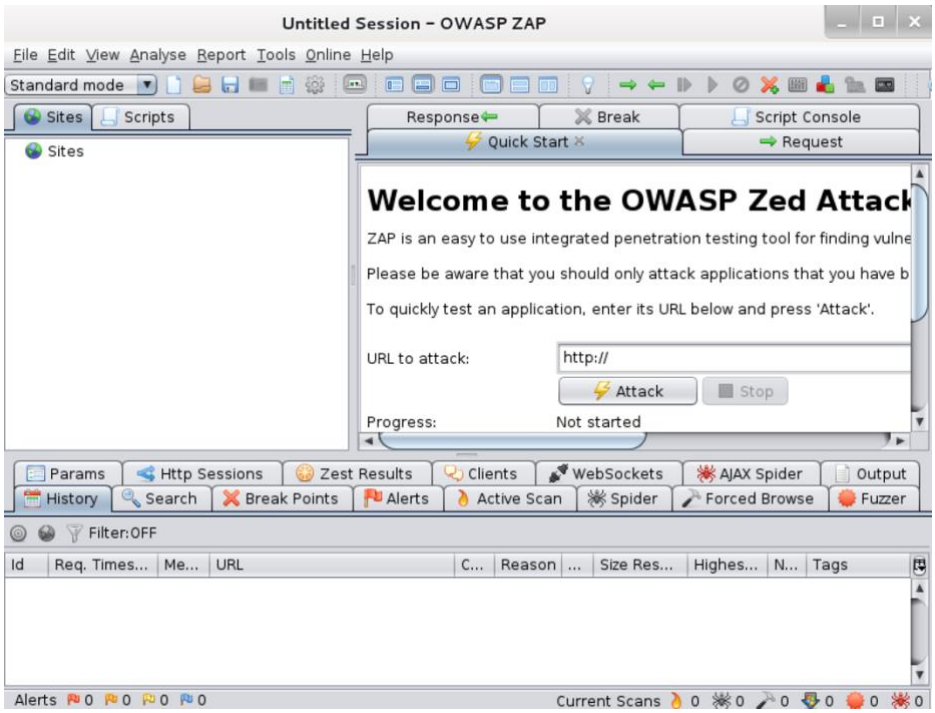



Gambar 2. 32 Contoh Penggunaan Nmap

### 2.13.8 OWASP ZAP

*Zed Attack Proxy* (ZAP) merupakan sebuah aplikasi untuk menemukan *vulnerabilities* dalam suatu *web applications* yang menyediakan *scanner* otomatis. Ketika digunakan sebagai *server proxy*, hal ini dapat memungkin pengguna untuk memanipulasi berbagai hal yang melewatinya, termasuk lalu lintas yang menggunakan https (Kusuma, 2022). *Zed Attack Proxy* (ZAP)

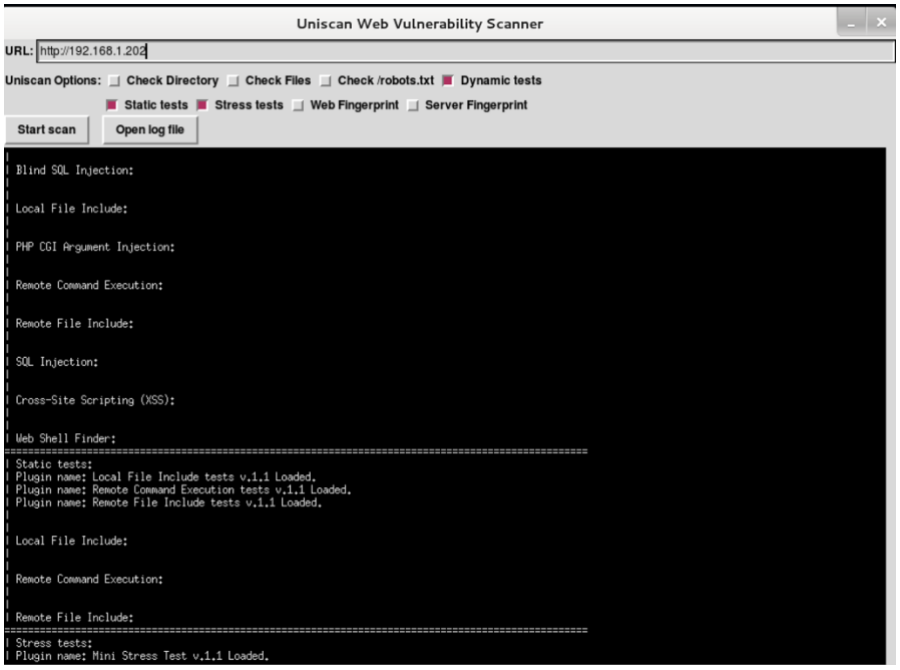
bersifat *open source*. Setelah ter*install*, masukkan alamat *web* yang akan dijadikan target kemudian tekan tombol *attack* (Wisanggeni, 2021). *Vulnerability Scanning* menggunakan *tool OWASP ZAP* dipaparkan pada sub bab 4.2.2.3.



Gambar 2. 33 OWASP ZAP

### 2.13.9 Uniscan

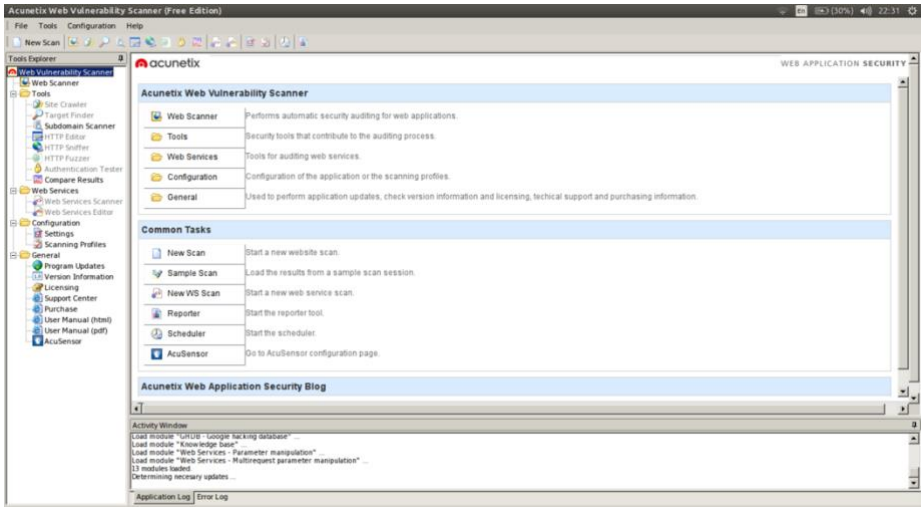
Uniscan adalah pemindai kerentanan *Remote File Include* (RFI), *Local File Include*, dan *Remote Command Execution Vulnerability Scanner* (Dougpoer, 2015), atau secara sederhana dapat disebut sebagai alat *scanner* kerentanan aplikasi *web* yang tersedia pada sistem operasi *Kali Linux* (Andria et al., 2021). Uniscan dijalankan dengan menuliskan perintah ‘uniscan -u alamat -qweds’, atau dapat menjalankan perintah ‘uniscan -h’ untuk dapat memunculkan fungsi atau perintah yang dapat dijalankan. Penggunaan *tool* ini dijelaskan pada sub bab 4.2.2.4.




Gambar 2. 34 Contoh Penggunaan Uniscan

### 2.13.10 Acunetix

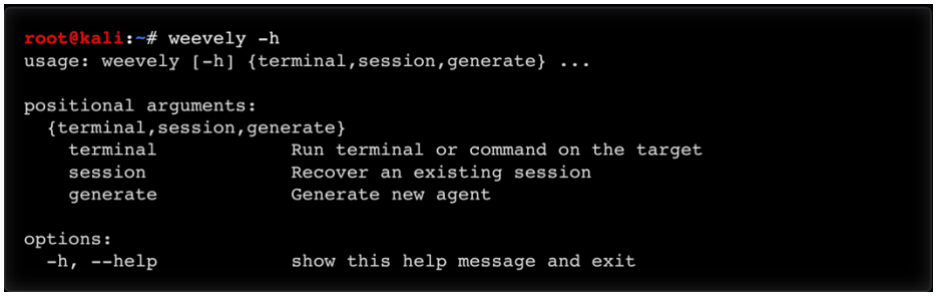
Acunetix adalah *tools* yang digunakan untuk melakukan *vulnerability scanning* dalam upaya untuk mencari atau mendeteksi celah kerentanan SQL *injection* dan XSS (Ula, 2019). Acunetix digunakan dengan memasukkan alamat target ke dalam acunetix yang dapat diakses melalui browser, untuk kemudian dapat dilakukan pemindaian untuk mendapatkan hasil dari kerentanan. Pada penelitian ini, penerapan acunetix dapat dilihat pada sub bab 4.2.2.5




Gambar 2. 35 Contoh Penggunaan Acunetix

### 2.13.11 Weevely

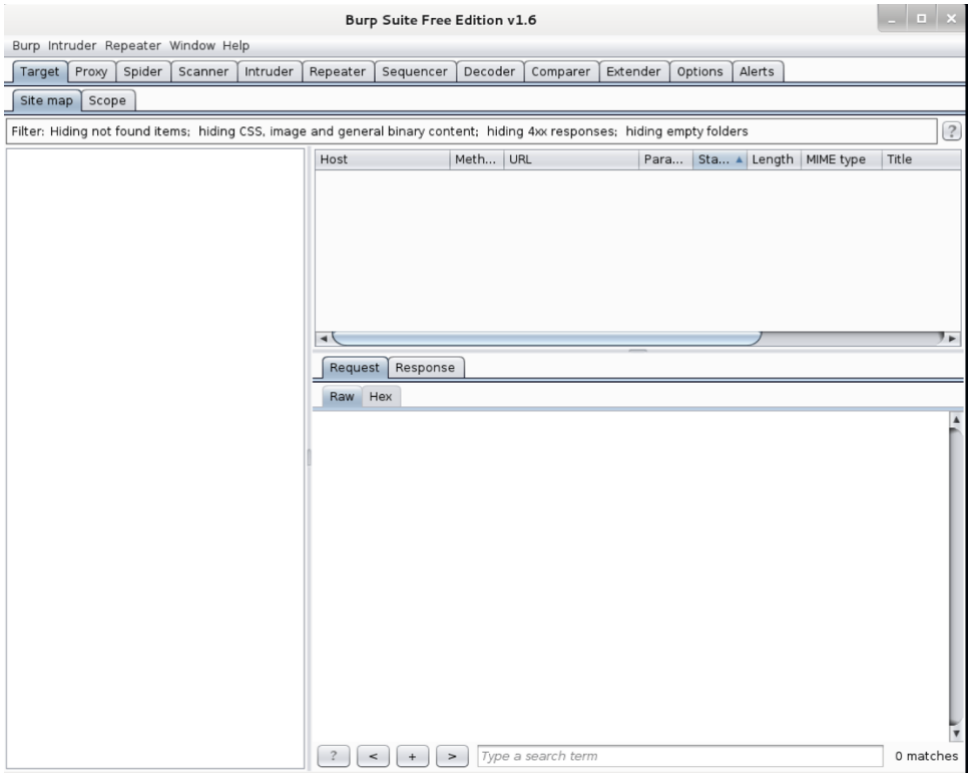
*Weevely* adalah *shell web* yang dirancang untuk melakukan tindakan pasca eksploitasi yang dapat diperluas melalui jaringan saat *runtime*, dengan lebih dari 30 modul untuk membantu berbagai tugas seperti, tugas administratif, memelihara akses, memberikan kesadaran situasional, meningkatkan hak istimewa, dan menyebar ke jaringan target (kali.org, n.d.). Untuk penerapannya, install *weevely* terlebih dahulu. Setelah itu, install dependensi dari *weevely* dengan perintah '#apt-get install python-prettytable python-mako python-dateutil python-socks python-yaml python', setelah itu *generate backdoor* dari *weevely* menggunakan perintah '#python weevely.py generate <password> <output-backdoor>, kemudian *upload* file output *weevely* ke *website* yang telah di siapkan. Setelah itu, masuk pada proses *remote weevely* '#python weevely.py https://website/path/weevely-backdoor.php' (Idfaris, 2020). Pada penelitian ini, *weevely* masuk ke dalam tahapan *post exploitation* yang dapat dilihat pada sub bab 4.2.4.




Gambar 2. 36 Cara Menggunakan Weevely

### 2.13.12 Burp Suite

*Burp Suite* adalah *platform* terintegrasi untuk melakukan pengujian keamanan aplikasi *web*. Berbagai alat didalamnya bekerja sama untuk mendukung seluruh proses pengujian, mulai dari pemetaan awal dan analisis permukaan serangan aplikasi, hingga menemukan dan mengeksploitasi kerentanan keamanan yang ditemukan (kali.org, 2023). *Tools* ini juga dapat digunakan untuk mencegat secara default protocol HTTP yang dkirim (*request*) dan diterima (*response*) oleh *browser* melalui jalur proxy. Untuk langkahnya, pertama dapat membuka *Burp Suite* kemudian pilih menu proxy, kemudian akses *browser*, masukkan IP dan *port* yang ada pada menu proxy di *Burp Suite*. Pilih menu *manual proxy configuration* dan centang bagian *also use this proxy for* FTP dan HTTPS, akses sebuah *website* melalui *browser*, kemudian dapatkan *PortSwigger CA* melalui situs https://burp dan pilih menu CA *Certificate*. Pada *browser*, klik *preference* dan pilih menu *view certificates*, lalu import file terdownload (Ilmu Bersama, 2021). *Burp Suite* diciptakan oleh perusahaan bernama *Portswigger* dengan tujuan untuk menjadi *toolkit all-in-one*, serta fitur yang dapat ditingkatkan dengan menginstall *BApps*, yaitu *add-on*-nya(Fathurrachman, 2023). Penerapan *Burp Suite* pada penelitian ini dapat dilihat pada tahapan *exploitation* di sub bab 4.2.3.




Gambar 2. 37 Cara Menggunakan Burp Suite

## 2.14 Literatur Sejenis

**Tabel 2. 7** Literatur Sejenis

| No. | Judul Penelitian | Nama Peneliti | Tahun | Teknik Pengujian | Jenis Pengujian | *Tools* | Jumlah *Tools Vulnerability Scanning* | Pengujian |
|---|---|---|---|---|---|---|---|---|
| 1 | *Analysis and Impact of Vulnerability Assessment and Penetration Testing*(Khera et al., 2019) | Yugansh Khera, Deepansh Kumar, Sujay, Nidhi Garg Department | 2019 | *Blackbox-testing* | *Vulnerability Assestment and Penetration Testin* | OWASP Top 10 | *1* | *Vulnerability Scanning, Penetration Testing* |
| 2 | PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY | Rama Sahtyawan | 2019 | *Blackbox-testing* | *Vulnerability Assestment and Penetration Testing* | *Kali Linux, DbVisualizer* | *1* | *Penetration Testing dengan* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING) (Sahtyawan, 2019) | | | | | | | *Metode Zero Entry Hacking (ZEH)* |
| 3 | ANALISIS DAN PENGUJIAN KERENTANAN SISTEM INFORMASI PERPUSTAKAAN (Nur, 2019). | Achmad Nur Sholeh, Muhammad Subagja Sastra Wardaya | 2019 | *Blackbox-testing* | *Vulnerability Assestment and Penetration Testin* | NMAP, OWASP ZAP, dan Accunetix | 2 | *Penetration Testing dengan Metode Zero Entry Hacking (ZEH)* |
| 4 | VULNERABILITY ASSESSMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB (Mira Orisa & Ardita, 2021) | Mira Orisa, Michael Ardita | 2021 | *Blackbox-testing* | *Vulnerability Assessment* | Nmap | 1 | *Vulnerability Assessment* |
| 5 | PEMERINGKATAN RISIKO KEAMANAN SISTEM JARINGAN KOMPUTER POLITEKNIK KOTA MALANG MENGGUNAKAN CVSS DAN (Retna Mulya & Tarigan, 2018) | Betta Wahyu Retna Mulya, Avinanta Tarigan | 2018 | *Blackbox-testing* | *Vulnerability Scoring* | *CVSS, FMEA, Nessus* | *1* | *Vulnerability Scoring* |
| 6 | NIST Internal Report NIST IR 8409 Measuring the Common Vulnerability Scoring System Base Score Equation (Mell et al., 2022) | Mell, Peter Dugal, Dave Casotto, Francesco Nordwall, Phillip Sommerfeld, Daniel | 2022 | Uji Validitas | - | *Common Vulnerability Scoring System* | - | *CVSS dan Sistem Penilaian Konsisten Terdekat* |
| 7 | ANALISIS KEAMANAN | Febri Al Fajar | 2020 | *Black-box testing* | *Pengujian Aplikasi Web* | *Acunetix, Launch* | *1* | *Penetration Testing* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY (Al Fajar, 2020) | | | | | *Attack HTTP Editor* | | |
| 8 | IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK (Kusuma, 2022) | Gregorius Hendita Artha Kusuma | 2022 | *Black-box testing* | *Vulnerability Scanner* | *OWASP ZAP* | *1* | *Penetration Testing* |

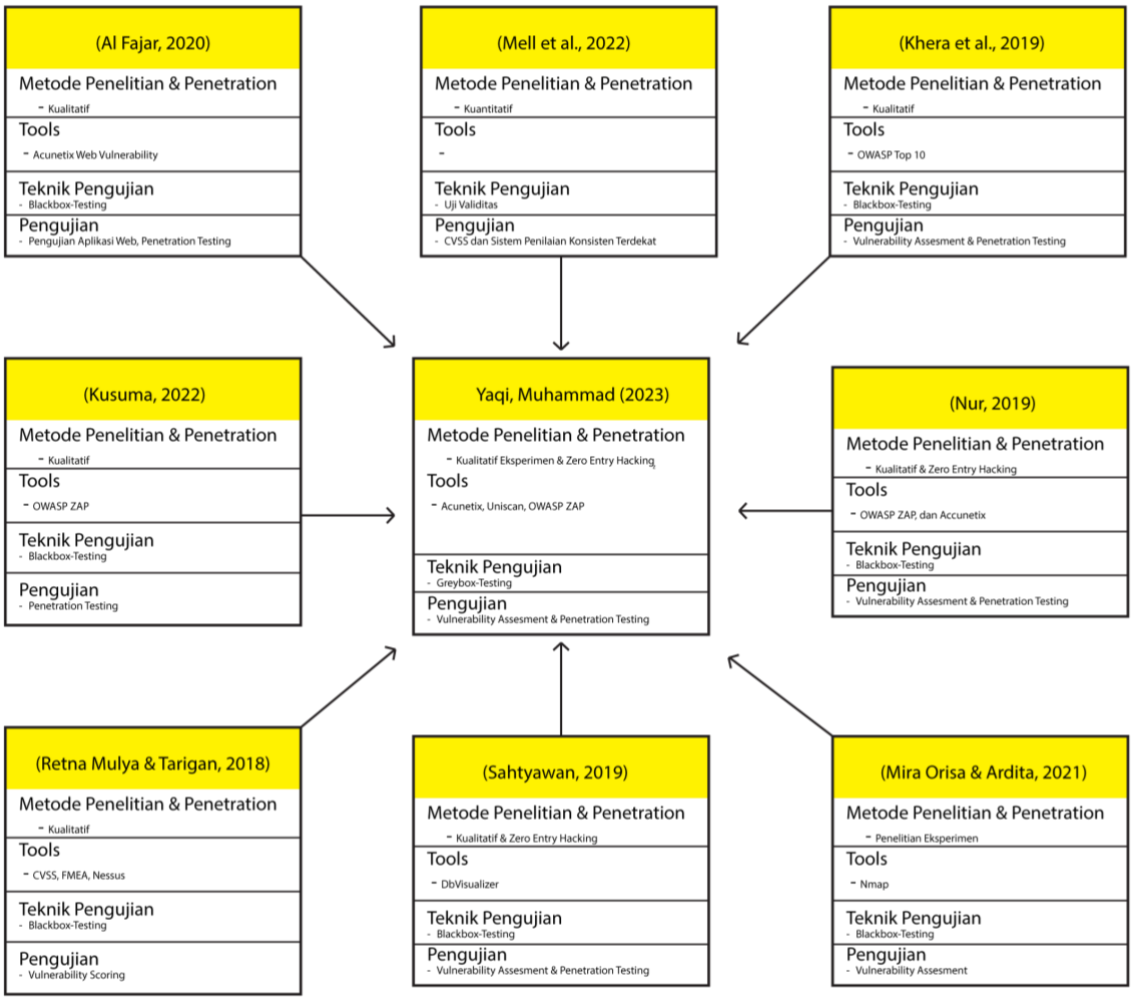
Berdasarkan 8 studi literatur sejenis yang telah penulis paparkan, penulis membandingkan penelitian penulis dengan penelitian sebelumnya. Berikut adalah kelebihan penelitian ini dibandingkan penelitian sebelumnya:

1. Merujuk pada paper dengan judul Penerapan *Zero Entry Hacking* di dalam *Misconfiguration* Pada VAPT oleh (Sahtyawan, 2019), penulis menggunakan metode *Zero Entry Hacking* sebagai metode *penetration testing*, karena beberapa penelitian sebelumnya yang diketahui menggunakan metode ini, mendapatkan hasil yang cukup efektif untuk melakukan *penetration testing*.
2. Penulis menggunakan beberap *tools* yang merujuk pada beberapa penelitian sebelumnya, yang kemudian penulis rangkum dan susun kedalam tahapan penelitian yang diantaranya, *Who* is, *E-mail* Harvester, *What Web, CXSecurity, Google Hacking Database + Google Dorking*, Terminal, Nmap, OWASP ZAP, Uniscan, Acunetix, Weevely, *Burp Suite* dan Microsoft Word.
3. Untuk memudahkan pencatatan terkait tingkatan kerentanan yang ditemukan, berdasarkan penelitian sebelumnya oleh Retna Mulya & Tarigan (2018), serta penelitian yang berjudul "NIST Internal Report NIST IR 8409 Measuring the Common Vulnerability Scoring System

Base Score Equation" oleh Mell et al. (2022), sehingga penelitian ini akan menggunakan *Common Vulnerabiliry Scoring System*.

4. Jenis penelitian yang dilakukan oleh penulis merujuk kepada beberapa penelitian terdahulu untuk dapat mendapatkan hasil yang baik. Pada penelitian ini, penulis menggunakan jenis penelitian eksperimen, dimana penelitian eksperimen yang dimaksud adalah *Pre-Experimental Design* dengan jenis *One Shot Case Study* karena dalam penelitian ini hanya terdapat satu kelompok yang diberikan *treatment* atau perlakukan serta tidak ada kelompok pembanding, sehingga kelompok yang diberikan *treatment* atau perlakukan tersebut langsung diukur untuk dapat diketahui hasilnya.
5. Penelitian ini menggunakan tiga *tools* (*Uniscan, OWASP ZAP,* dan *Acunetix*) pada tahapan *vulnerability assessment* untuk dapat memperkuat hasil dari pemindaian kerentanan, dibandingkan beberapa penelitian lainnya yang hanya menggunakan satu atau dua *tools* untuk melakukan *vulnerability assessment* yang dapat dilihat pada tabel 2.7.
6. Teknik pengujian pada penelitian ini menggunakan teknik pengujian *Greybox-testing* karena peneliti mendapatkan beberapa informasi terkait objek penelitian yang mampu membantu proses penelitian.
7. Penelitian ini termasuk kedalam jenis *Network Penetration Testing External*.
8. *Website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan yang dijadikan objek penelitian termasuk kedalam jenis *website* dinamis.

Visualisasi *mapping* terkait penelitian yang penulis lakukan dengan peneletian terdahulu yang sejenis, penulis tampilkan pada gambar berikut.




Gambar 2. 38 Visualisasi Mapping Literatur Sejenis

# BAB III
# METODE PENELITIAN

Penelitian ini menggunakan metode atau jenis penelitian eksperimen dengan melakukan pengujian pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan. Penelitian eksperimen yang penulis gunakan adalah penelitian *Pre-Experiment Design* dengan jenis *One Shot Case Study,* hal ini dikarenakan penelitian ini hanya terdapat satu kelompok yang diberikan *treatment* atau perlakukan serta tidak ada kelompok pembanding, sehingga kelompok yang diberikan *treatment* atau perlakukan tersebut langsung diukur untuk dapat diketahui hasilnya.

Pada tahap pengumpulan data dilakukan dengan menggunakan studi pustaka dan studi lapangan. Kemudian metode yang digunakan untuk uji dan analisis menggunakan *Vulnerability Assessment and Penetration Testing* (VAPT) dengan *Zero Entry Hacking* sebagia metode yang digunakan untuk *penetration testing*.

Studi lapangan dilakukan dengan menggunakan metode wawancara dan observasi terhadap pihak Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan. Kemudian studi pustaka dilakukan dengan mencari informasi dari berbagai sumber. Pada pengimplementasiannya, *penetration testing* yang akan dilakuukan menggunakan metode *Zero Entry Hacking* (ZEH) melalui 4 tahapan yaitu, melakukan pengintaian sistem (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi Celah Kerentanan (*Exploitation*), dan Pasca Eksploitasi (*Post Exploitation*). Kemudian untuk pengukuran kerentanan, penulis menggunakan *Common Vulnerability Scoring System* (CVSS) untuk memaparkan tingkatan celah kerentanan yang ditemukan.

Uji *Vulnerability Assessment* dan *Penetration Testing*, serta pengukuran tingkatan kerentanan yang ditemukan akan dibahas pada BAB IV. ANALISI DAN IMPLEMENTASI SISTEM.

## 3.1 Metode Pengumpulan Data

Penelitian ini menggunakan data dan informasi yang diperoleh dari berbagai sumber sebagai acuan, untuk itu beberapa metode diperlukan untuk mendapatkan informasi mengenai kerentan sistem pada aplikasi berbasis *website* yang dimiliki oleh Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan. Selain itu, penulis juga mengumpulkan data mengenai objek penelitaian.

### 3.1.1 Studi Lapangan

Penelitian ini menggunakan studi lapangan untuk mendapatkan rumusan masalah secara akurat. Adapun dalam penelitian ini peneliti melakukan observasi dan wawancara terhadap Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, sebagai berikut.

#### 3.1.1.1 Oberservasi

Observasi dilakukan dengan mengamati secara langsung objek penelitian yang ada pada Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan yang secara spesifik dapat dijabarkan sebagai berikut:

Tempat : Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

Alamat : Jl. Raya Serpong Km.16 Cilenggang, Kec. Serpong, Kota Tangerang Selatan, Banten 15310

*Website* : https://dpmptsp.tangerangselatankota.go.id/

Waktu : Oktober 2022 – Februari 2023

Hasil : Mendapatkan berbagai informasi mengenai Dinas Penanaman Modal dan PTSP Kota

Tangerang Selatan seperti informasi mengenai *website* dan topologi jaringan.

#### 3.1.1.2 Wawancara

Untuk memperkuat observasi, penulis juga melakukan wawancara dengan salah satu staff Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan bernama Bapak Sru Wahyudi dan Bapak Ardan, dengan hasil wawancara yang akan dilampirkan pada halaman lampiran. Pertanyaan yang penulis ajukan bersifat teknis yang mengacu pada topik keamanan pada aplikasi berbasis *web* miliki pihak yang bersangkutan. Proses wawancara ini dilakukan melalui percakapan *via Whatsapp* dengan hasil diketahui bahwa belum pernah terjadi serangan pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan, serta telah diterapkan sebuah sistem untuk melakukan pengamanan yaitu WAF (*Web Application Firewall*) dan *Honeypot*.

### 3.1.2 Studi Pustaka

Metode pengumpulan data studi pustaka yang dilakukan adalah dengan mencari informasi dari berbagai sumber seperti buku, *e*-book, *web*, dan studi literatur sejenis.

#### 3.1.2.1 Studi Literatur

Data-data serta informasi yang digunakan sebagai studi literatur dengan mempelajari dan mengumpulkan berbagai materi yang erat kaitannya dengan keamanan sistem informasi. Studi literature dapat dilihat pada sub bab 2.13 Literatur Sejenis.

## 3.2 Metode Pengujian dan Analisis

Metodologi yang digunakan dalam pengujian dan Analisis pada penelitian ini adalah metode *Zero Entry Hacking* (ZEH). Adapun tahapan yang akan dilakukan yaitu: Pengintaian Sistem (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi Celah Kerentanan (*Exploitation*), dan Pasca Eksploitasi (*Post Exploitation*).

Untuk mendapatkan nilai dengan standar umum yang banyak digunakan dalam pengujian ini, penulis akan melakukan pengukuran nilai-nilai kerentanan menggunakan *Common Vulnerabilty Scoring System* (CVSS).

### 3.2.1 Roadmap Penelitian

Penjelasan mendetail terkait penelitian penulis jabarkan dalam tabal *Roadmap* yang dapat dilihat pada tabel berikut:

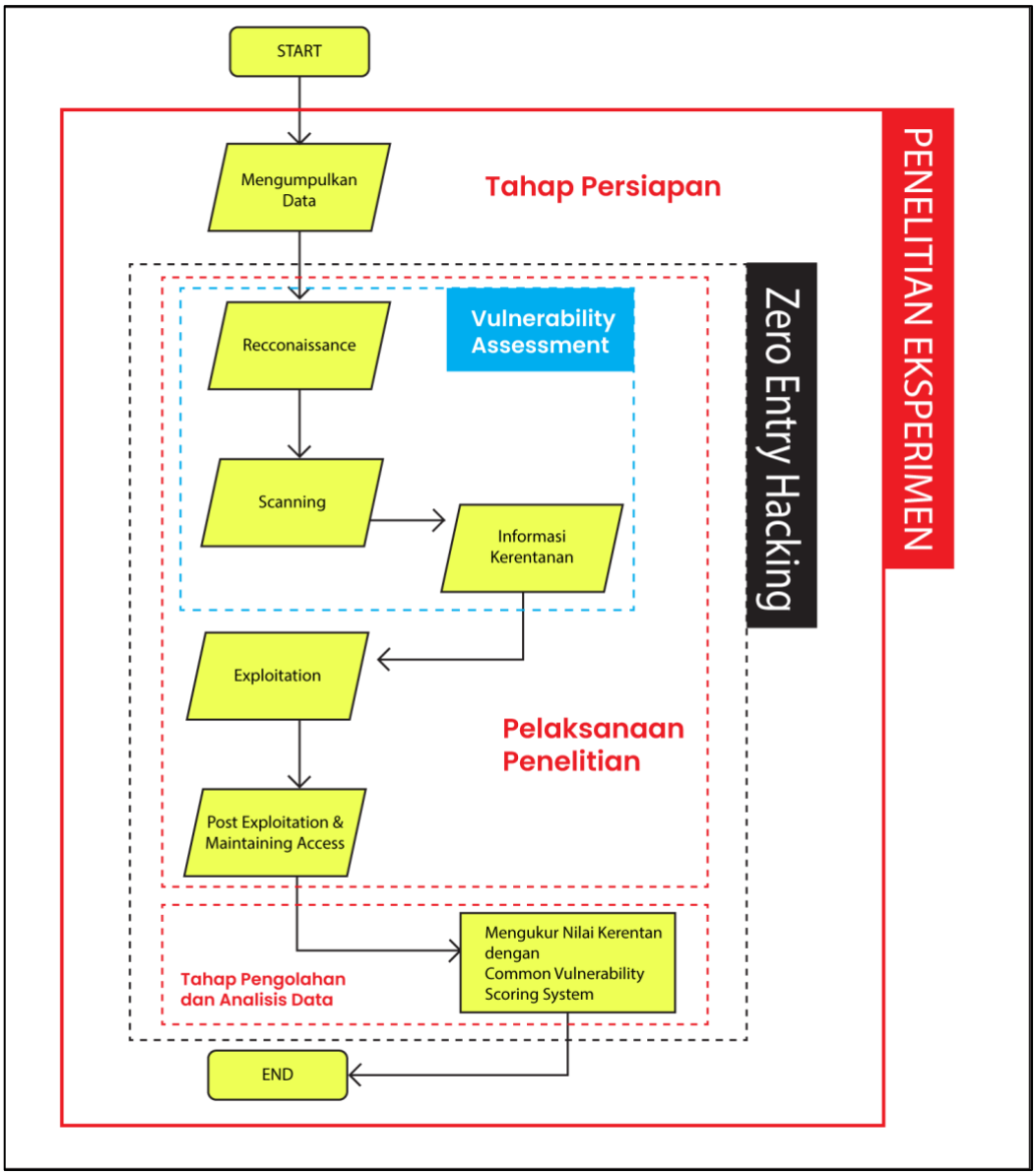
**Tabel 3. 1 *Roadmap* Metode Uji *Zero Entry Hacking* Pada Penelitian ini**

| No | Tahap | Keterangan | Field | Tools | Tujuan |
|---|---|---|---|---|---|
| 1 | *Reconnaisance* | Pada tahap ini, penulis menempatkan dirinya sebagai *hacker* untuk melakukan pengumpulan informasi secara *external*. Selain itu, beberapa informasi yang telah penulis dapatkan melalui wawancara dengan pihak terkait dimanfaatkan oleh penulis sebagai penguat informasi. | Domain | *Who is* | Mencari tahu informasi mengenai domain Dinas Penanaman Modal dan PTSP Kota Tangerang Seelatan |
| | | | E-mail | *E-mail Harvester* | Menggali informasi mengenai akun *e-mail* yang tersebar dalam mesin pencari |
| | | | *Framework* | *What Web* | Mengidentifikasi komposisi penyusunan *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan |
| | | | *Versi Rentan* | *CXSecurity* | Menemukan kerentanan dari versi aplikasi yang digunakan |
| | | | *Dorking* | *Google Hacking Database* + *Google Dorking* | Menemukan daftar celah yang tersedia dalam GHDB, untuk ditindak lanjuti dengan pencarian dalam mesin pencari Google |
| 2 | *Scanning* | Pada tahap ini, penulis berperan sebagai *hacker* untuk mencari celah | *Ping* | Terminal | Mengetahui apakah *web* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dapat diakses dari luar atau tidak |

| | | | | | |
|---|---|---|---|---|---|
| | | kerentanan yang ada untuk kemudian dapat dilakukan eksploitasi. | *Port Scanner* | NMAP | Mencari *Port* yang terbuka dan tidak dipergunakan |
| | | | *Vulnerability Scanner* | OWASP ZAP, Uniscan dan Acunetix | Mencari celah kerentanan yang ada |
| 3 | *Exploitation* | Pada tahap ini, penulis sebagai seorang *hacker* memanfaatkan celah kerentanan yang diketahui untuk dieksploitasi, dengan memanfaatkan informasi yang didapatkan secara *external* ataupun infromasi dari pihak terkait. Maka dalam hal ini, pengujian ini termasuk kedalam *greybox-testing*. | Eksploitasi Berbasis *Web* | Burp Suite | Menguji kerentanan yang didapat dari tahapan sebelumnya |
| 4 | *Post Exploitation* | Pada tahap ini, penulis berperan sebagai *hacker* (*whitehat*), karena nantinya kerentanan yang ditemui dan di dokumentasikan akan diberikan juga kepihak yang terkait untuk dapat dilakukan perbaikan. | Pembuatan *Backdoor* | Weevely | Mempertahankan akses yang didapat |
| | | | Pelaporan Akhir | Microsoft Word | Melaporkan hasil uji |

## 3.3 Kerangka Penelitian

Dalam melakukan penelitian, penulis melakukan tahapan-tahapan kegiatan yang tertuang dalam rencana kegiatan penelitian, meliputi metode pengujian dan analisis sebagai berikut.




Gambar 3. 1 Rencana Penelitian

### 3.3.1 *Reconnaisance*

*Reconnaisance* adalah tahapan pertama yang bertujuan untuk menggali informasi sebanyak mungkin mengenai objek yang di uji. Adapun beberapa *tools* yang dapat digunakan sebagai berikut:

1. *WHO IS*, akan digunakan untuk mencari alamat IP dan informasi berharga seperti pencatat *domain*, status, tanggal kadaluarsa, dan nama *server* DNS.

2. *The Harvester,* digunakan untuk mendapatkan informasi *email, subdomain, host,* dan lain sebagainya.
3. *What Web,* digunakan utnuk mendapatkan alamat *email*, nomor versi, ID akun, modul kerangka kerja *web*, kesalahan SQL, dan lain sebagainya.
4. *CXSecurity,* akan digunakan sebagai panduan identifikasi terkait objek yang akan di uji melalui *database* yang ada pada *CXSecurity*.
5. *Google Hacking Database* + *Google Dorking*, akan digunakan untuk melakukan pencarian informasi yang tidak mudah untuk terlihat oleh publik untuk kemudian digunakan dalam upaya untuk menemukan kerentanan didalamnya.

### 3.3.2 Pemindaian (*Scanning*)

Setelah pengintaian (*reconnaisance*), langkah selanjutnya adalah melakukan pemindaian yang dalam hal ini dibagi menjadi tiga tahapan yaitu:

1. Menentukan mampu atau tidaknya objek tersebut untuk di *ping* atau untuk mengetahui apakah objek tersebut terhubung dengan jaringan atau tidak, apakah objek hanya dapat diakses melalui jaringan lokal atau dapat diakses dari luar, bagus atau tidaknya kualitas koneksi objek, berapa durasi yang diperlukan objek untuk membalas *ping*, *bytes* yang dikirimkan hilang atau dapat diterima, serta apakah objek dapat melakukan *ping* pada dirinya sendiri.
2. *Port scanning* sistem menggunakan NMAP untuk memonitor dan sebagai alat *penetration testing*.
3. Pemindaian menggunakan *vulnerability scanner tools* OWASP ZAP, Uniscan, dan Acunetix untuk mencari tau kerentanan yang ada.

### 3.3.3 Eksploitasi Celah Kerentanan (*Exploitation*)

Pada tahap ini peneliti akan melakukan penyerangan melalui *tools* Nmap, OWASP ZAP, dan *Burp Suite* untuk menindak lanjuti celah kerentanan yang ditemukan.

### 3.3.4 Pasca Eksploitasi (*Post Exploitaiton*)

Pada tahap ini, *Weevely* adalah *tools* yang akan digunakan untuk melakukan pengamanan terkait akses yang didapatkan dengan membuat *backdoor*, dan setelahnya akan dibuat laporan mengenai hasil pengujian yang telah peneliti lakukan.

# BAB IV
# ANALISIS DAN IMPLEMENTASI SISTEM

## 4.1 Analisis Alat Kebutuhan Pengujian

Dalam penelitian ini, alat yang digunakan terdiri atas beberapa perangkat keras (*hardware*), perangkat lunak (*software*), dan *tools* sebagai berikut.

*a. Hardware*

Perangkat keras (*hardware*) yang digunakan pada penelitian terdiri dari sebuah Laptop dengan *Processor* 2,3 GHz Dual-Core Intel Core i5, RAM 16 GB, dan SSD sebesar 256 GB.

**Tabel 4. 1** Perangkat Keras (Hardware) Penelitian

| No. | Nama Perangkat Keras | Spesifikasi |
|---|---|---|
| 1 | *Processor* | 2,3 GHz Dual-Core Intel Core i5 |
| 2 | RAM | 16 GB |
| 3 | SSD | 256 GB |

*b. Software*

Perangkat lunak (*software*) yang digunakan pada penelitian ini terdiri dari *Operating System* MacOS BigSur v11.7.4, Kali Linux, dan Oracle VM Virtual Box v7.0.6.

**Tabel 4. 2** Perangkat Lunak (Software) Penelitian

| No. | Nama Perangkat Lunak | Versi |
|---|---|---|
| 1 | *Operating System* (OS) | macOS BigSur v11.7.4, dan Kali Linux |
| 2 | *Application Software* | Oracle VM Virtual Box v7.0.6 |

*c. Tools*

Penelitian ini menggunakan beberapa *tools* yang digunakan pada proses pengintaian (*Reconnaisance*), Pemindaian (*Scanning*), Eksploitasi (*Exploitation*), dan Pasca Eksploitasi (*Post Exploitation*) seperti, *Whatweb, Whois, theHarvester, CXSecurity, Google Hacking Database, OWASP ZAP, Uniscan, Acunetix, Burp Suite* dan *Weevely*.

**Tabel 4. 3** Tools yang digunakan untuk Penelitian

| No. | Tahapan | *Tools* | Fungsi |
|---|---|---|---|
| 1 | *ReconnaisMance* | *Whatweb, Whois, theHarvester, CXSecurity, Google Hacking Database* | Untuk mencari informasi mengenai hal-hal yang cukup penting seperti *email, domain, host* dan lain sebagainya. |
| 2 | *Scanning* | *Nmap, OWASP ZAP, Acunetix* | Untuk mencari *port* yang terbuka, dan mencari celah kerentanan yang ada. |
| 3 | *Exploitation* | *Burp Suite* | Untuk menguji kerentanan yang telah ditemukan. |
| 4 | *Post Exploitation* | *Weevely* | Mempertahankan akses yang telah didapatkan |

## 4.2 Implementasi Sistem

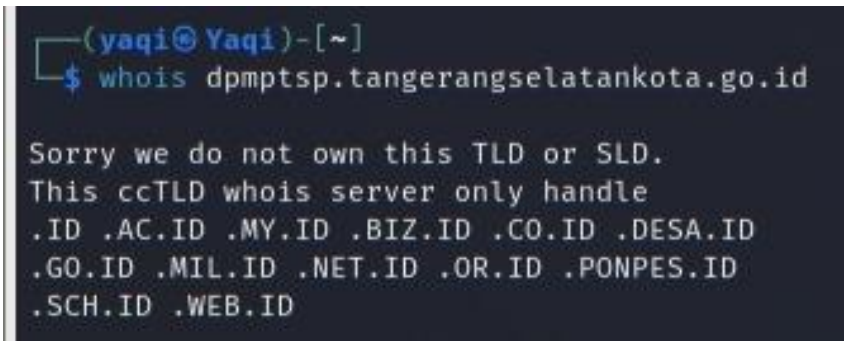
Pada tahap ini, peneliti akan menerapkan empat tahapan sesuai dengan metode *Zero Entry Hacking* yaitu, *Reconnaisance, Scanning, Exploitation,* dan *Post Exploitation* yang dilakukan pada tanggal 19 Mei 2023 sampai dengan 24 Mei 2023.

### 4.2.1 Tahap *Reconnaisance* (Pengintaian Target)

Dalam melakukan pengintaian target (*reconnaisance*), penelitian ini menggunakan beberapa *tools* untuk berusaha mendapatkan informasi yang dibutuhkan.

#### 4.2.1.1 *Who is*

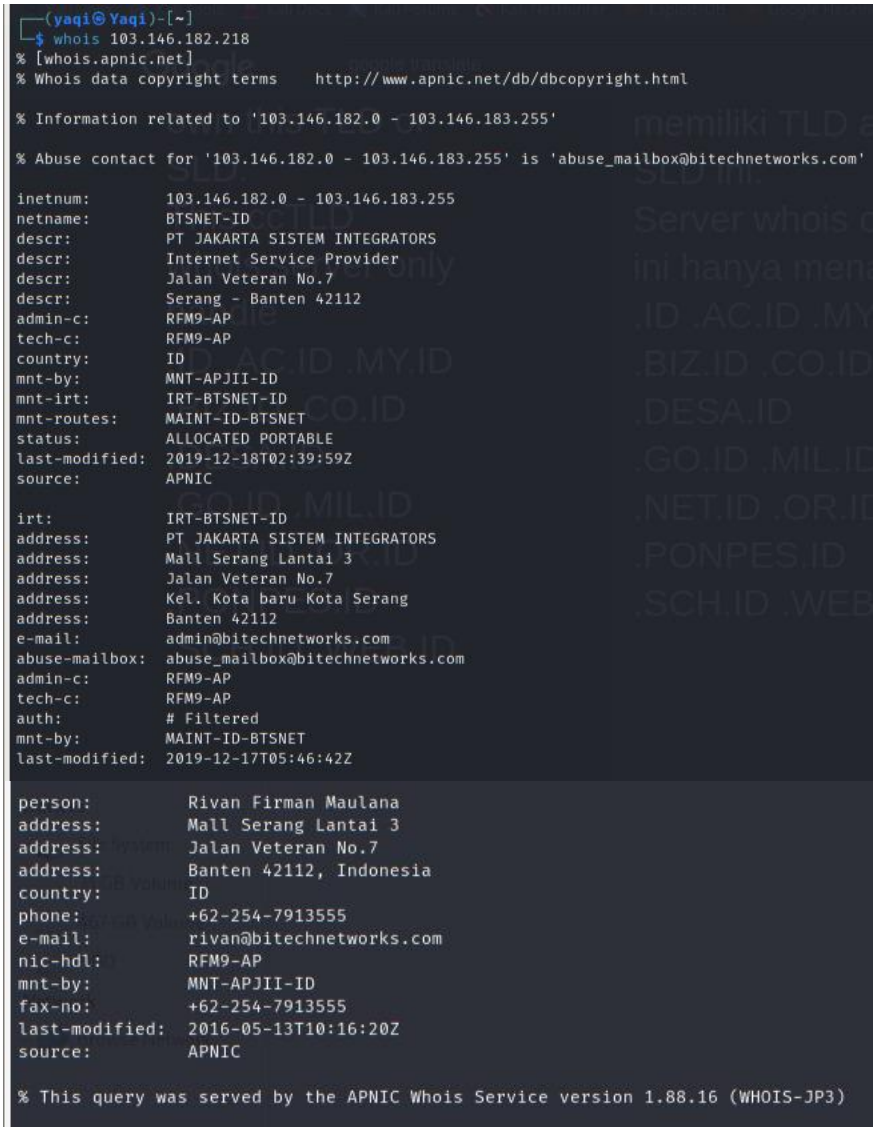
Pada tahap ini, *information gathering* pertama kali dilakukan menggunakan *Who is 'whois* dpmptsp.tangerangselatankota.go.id*'* untuk mendapatkan informasi sebagai berikut.




Gambar 4. 1 Hasil Who Is-1

Berdasarkan perintah di atas dengan melakukan pencarian berdasarkan alamat *email* dpmptsp.tangerangselatankota.go.id tidak dapat menampilkan hasil, karena hanya menangani .ID, .AC.ID, .MY.ID, .GO.ID, dan lain sebagainya.

Kemudian peneliti mencoba untuk melakukan pencarian informasi menggunakan alamat IP *website* dpmptps.tangerangselatankota.go.id yaitu '103.146.182.218', sebagai berikut.



```
┌──(yaqi㉿Yaqi)-[~]
└─$ whois 103.146.182.218
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.146.182.0 - 103.146.183.255'

% Abuse contact for '103.146.182.0 - 103.146.183.255' is 'abuse_mailbox@bitechnetworks.com'

inetnum:        103.146.182.0 - 103.146.183.255
netname:        BTSNET-ID
descr:          PT JAKARTA SISTEM INTEGRATORS
descr:          Internet Service Provider
descr:          Jalan Veteran No.7
descr:          Serang - Banten 42112
admin-c:        RFM9-AP
tech-c:         RFM9-AP
country:        ID
mnt-by:         MNT-APJII-ID
mnt-irt:        IRT-BTSNET-ID
mnt-routes:     MAINT-ID-BTSNET
status:         ALLOCATED PORTABLE
last-modified:  2019-12-18T02:39:59Z
source:         APNIC

irt:            IRT-BTSNET-ID
address:        PT JAKARTA SISTEM INTEGRATORS
address:        Mall Serang Lantai 3
address:        Jalan Veteran No.7
address:        Kel. Kota baru Kota Serang
address:        Banten 42112
e-mail:         admin@bitechnetworks.com
abuse-mailbox:  abuse_mailbox@bitechnetworks.com
admin-c:        RFM9-AP
tech-c:         RFM9-AP
auth:           # Filtered
mnt-by:         MAINT-ID-BTSNET
last-modified:  2019-12-17T05:46:42Z

person:         Rivan Firman Maulana
address:        Mall Serang Lantai 3
address:        Jalan Veteran No.7
address:        Banten 42112, Indonesia
country:        ID
phone:          +62-254-7913555
e-mail:         rivan@bitechnetworks.com
nic-hdl:        RFM9-AP
mnt-by:         MNT-APJII-ID
fax-no:         +62-254-7913555
last-modified:  2016-05-13T10:16:20Z
source:         APNIC

% This query was served by the APNIC Whois Service version 1.88.16 (WHOIS-JP3)
```

Gambar 4. 2 Hasil Who Is-2

Berdasarkan hasil perintah ini, didapatkan hasil informasi seperti nama yang terdaftar, alamat, nomor, nic-hdl, negara dan sumbernya. Selain itu, juga didapatkan data organisasi di dalamnya seperti *inetnum*, *netname*, alamat, *mnt-irt*, *mnt-routes*, *status*, *auth*, *last-modified*, dan lain sebagainya.

Peneliti juga melakukan pencarian melalui sumber lain yaitu melalui ipku.in dan bgp.he.net dengan alamat IP yang sama dan didapatkan hasil yang serupa sebagai berikut.

```
aut-num:        AS137342
as-name:        IDNIC-KOMINFOTANGSEL-AS-ID
descr:          DISKOMINFO TANGERANG SELATAN
descr:          Government / Direct Member IDNIC
descr:          Tangerang Selatan
country:        ID
admin-c:        RFM9-AP
tech-c:         RFM9-AP
mnt-by:         MNT-APJII-ID
mnt-irt:        IRT-BPTI-ID
mnt-routes:     MAINT-ID-BPTI-TS
import:         from AS38150 action pref=100; accept ANY
import:         from AS45298 action pref=100; accept ANY
export:         to AS38150 announce AS137342
export:         to AS45298 announce AS137342
default:        to AS45298 action pref=10;networks ANY
last-modified:  2018-04-13T04:30:07Z
notify:         rivan@bitechnetworks.com
remarks:        Send Spam & Abuse reports to: abuse@tangerangselatankota.go.id
source:         APNIC

irt:            IRT-BPTI-ID
address:        BPTI PEMKOT TANGSEL
address:        Bagian Pengelola Teknologi Informasi
address:        Jl. Maruga No. 1 Serua
address:        Ciputat Tangerang Selatan
e-mail:         aplahunnajat@tangerangselatankota.go.id
abuse-mailbox:  aplahunnajat@tangerangselatankota.go.id
admin-c:        AA1244-AP
tech-c:         AA1244-AP
auth:           # Filtered
mnt-by:         MNT-APJII-ID
last-modified:  2018-05-31T22:31:15Z
source:         APNIC

person:         Rivan Firman Maulana
address:        Mall Serang Lantai 3
address:        Jalan Veteran No.7
address:        Banten 42112, Indonesia
country:        ID
phone:          +62-254-7913555
e-mail:         rivan@bitechnetworks.com
nic-hdl:        RFM9-AP
mnt-by:         MNT-APJII-ID
fax-no:         +62-254-7913555
last-modified:  2016-05-13T10:16:20Z
source:         APNIC
```

Gambar 4. 4 Hasil Pencarian Dukungan Bgp.he.net

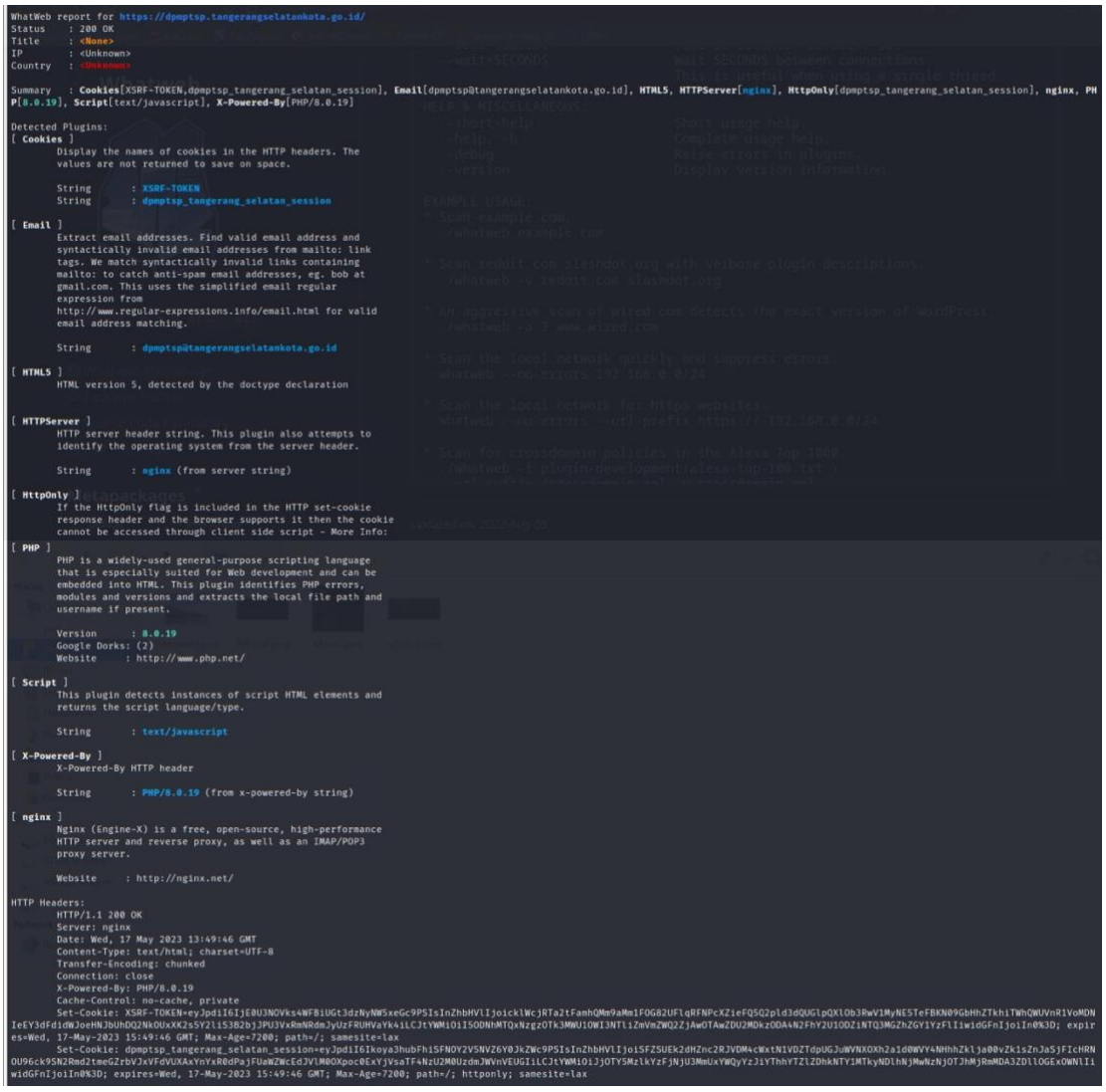
The IP : **103.146.182.218**
Location : South Tangerang,ID
Hostname :
ASN : AS137342 DISKOMINFO TANGERANG SELATAN

Gambar 4. 3 Hasil Pencarian Dukungan Ipku.in

#### 4.2.1.2 *What Web*

Selanjutanya, *information gathering* dilakukan dengan menggunakan perintah dari *Whatweb* ‘whatweb -v

dpmptsp.tangerangselatankota.go.id -a 3’ dengan hasil sebagai berikut.

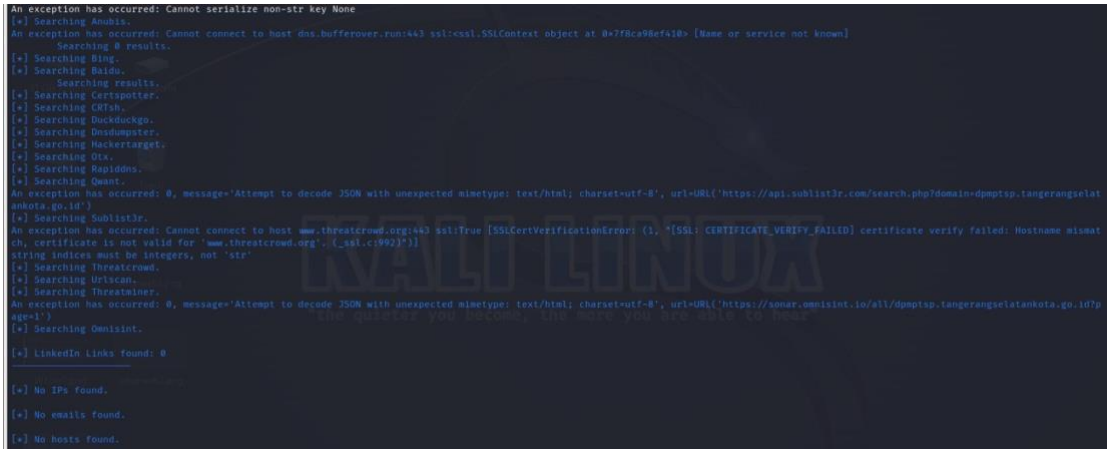



Gambar 4. 5 Hasil WhatWeb

Hasil yang didapatkan dari perintah *whatweb*, diketahui bahwa HTTP *Server* yang digunakan adalah *nginx*, dengan *email* yaitu dpmptsp@tangerangselatankota.go.id, serta menggunakan *Javascript*, HTML 5 dan PHP versi 8.0.19 untuk pembuatan *website*-nya.

#### 4.2.1.3 *The Harvester*

The Harvester selanjutnya digunakan untuk dapat menambahkan berbagai informasi penting lainnya dengan perintah ’theHarvester -d dpmptsp.tangerangselatankota.go.id -l 300 -b all’ sebagai berikut.

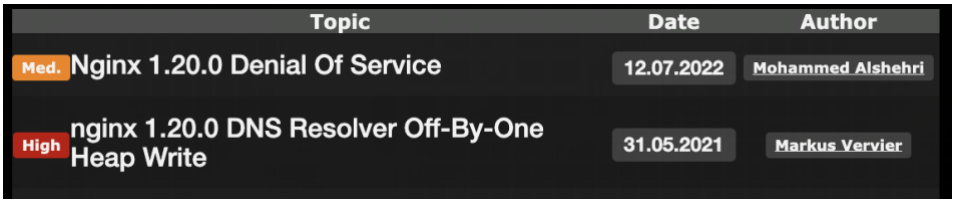



Gambar 4. 6 Hasil The Harvester

Pada The Harvester dengan perintah tersebut tidak dapat menemukan hasil terkait IP, *Email,* ataupun *Host* pada semua sumber yang ada dengan limit yang digunakan sebesar 300.

#### 4.2.1.4 *CXSecurity*

Berdasarkan informasi mengenai aplikasi *web* yang telah didapatkan sebelumnya, kerentanan dari versi aplikasi yang ditemukan sebagai berikut.



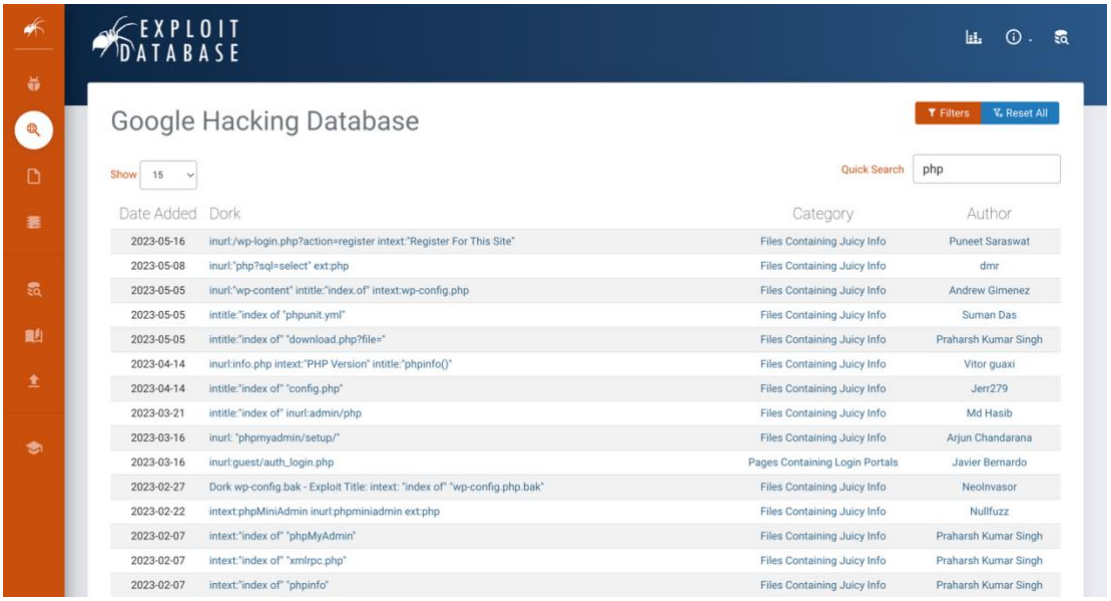
| Topic | Date | Author |
|---|---|---|
| Med. Nginx 1.20.0 Denial Of Service | 12.07.2022 | Mohammed Alshehri |
| High nginx 1.20.0 DNS Resolver Off-By-One Heap Write | 31.05.2021 | Markus Vervier |

Gambar 4. 7 Hasil Pengintaian CXSecurity Nginx

Diketahui bahwa *Nginx* 1.20.00 memiliki kerentanan *Denial of Service* dan DNS *Resolver Off-By-One Heap Write* yang dapat menyebabkan rusaknya fungsi.

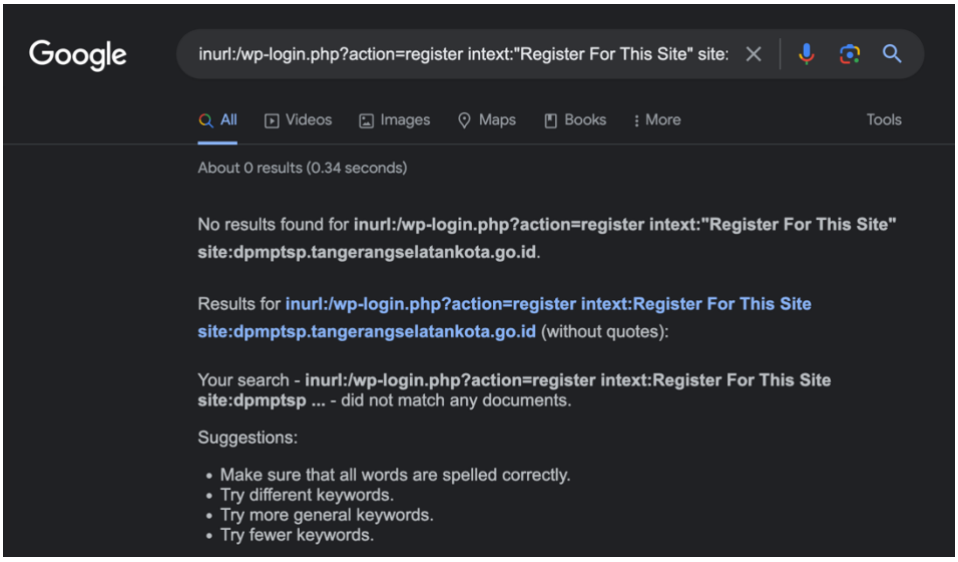
#### 4.2.1.5 *Google Hacking Database* + *Google Dorking*

Penambahan informasi dilakukan dengan memanfaatkan daftar celah yang tersedia dalam *Google Hacking Database* (GHDB) untuk kemudian dilanjutkan dengan pencarian menggunakan mesin pencarian *google.*




Gambar 4. 8 Daftar Dork PHP dalam GHDB

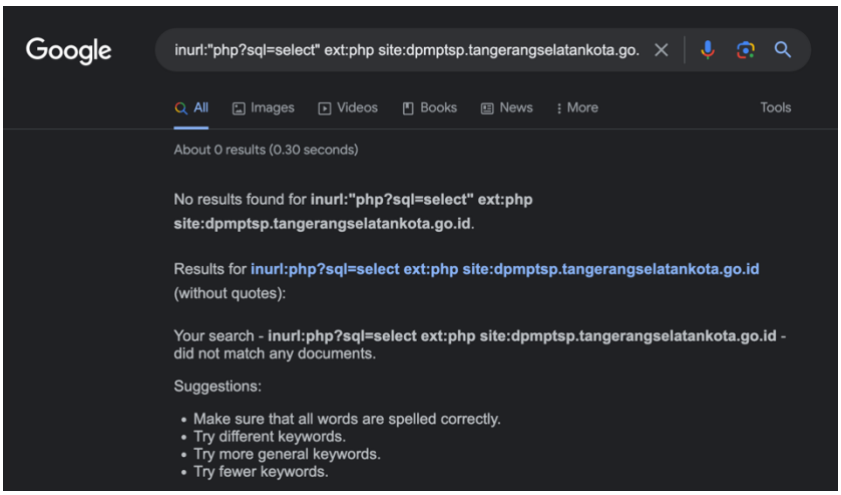
1. *Wp-login.php?action=register*




Gambar 4. 9 Wp-login.php?action=register

*Dork* yang diterbitkan pada16-05-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan *wp-login.php* yang tidak dilindungi. Kerentanan ini tidak ditemukan.

2. *Php?sql=select*

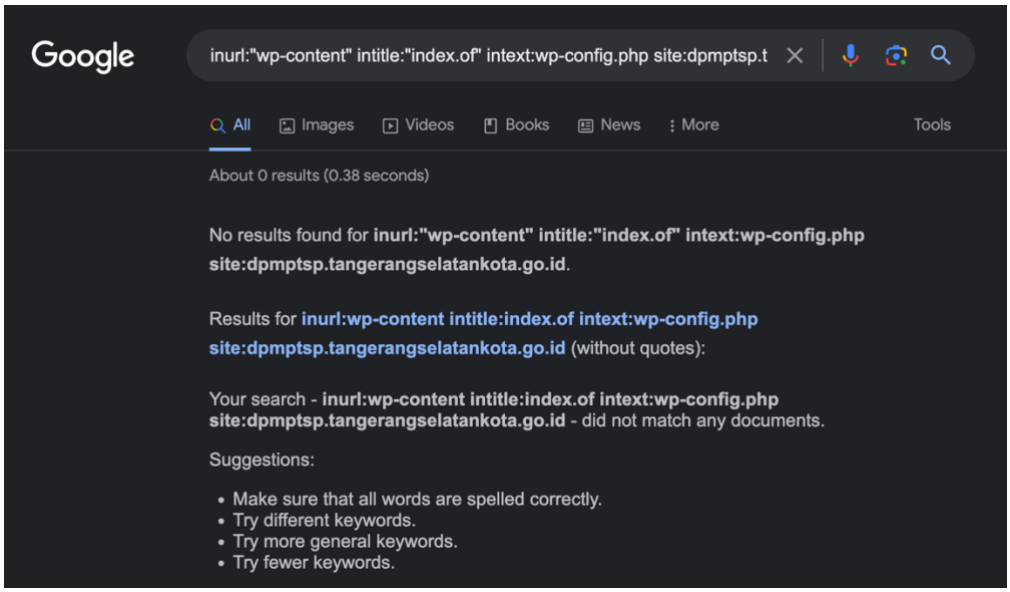



Gambar 4. 10 Php?sql=select

*Dork* yang diterbitkan pada 08-05-2023 ini merupakan suatu kerentanan yang menampilkan halaman

berisi file pengaturan yang tidak dilindungi. Kerentanan ini tidak ditemukan.

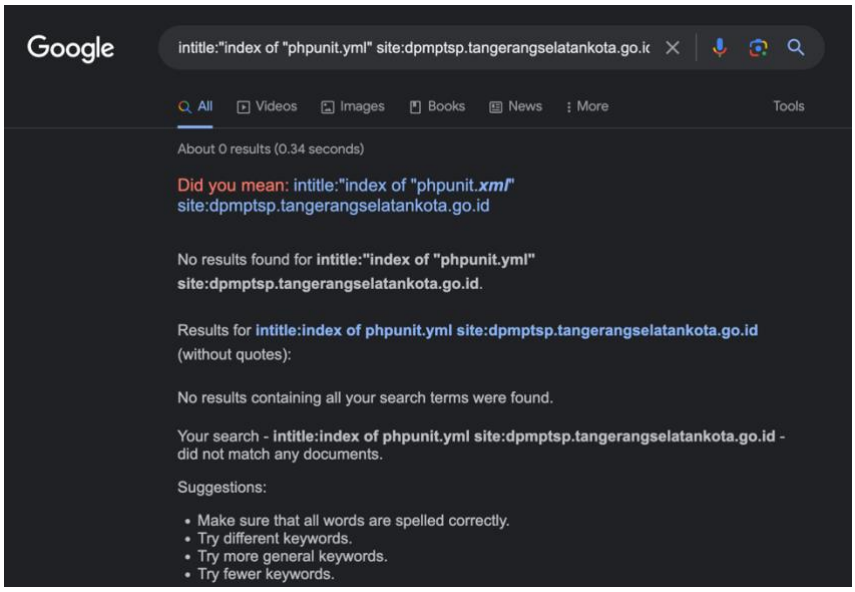
3. *Wp-config.php*




Gambar 4. 11 Wp-config.php

*Dork* yang diterbitkan pada 05-05-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan *wp-config.php* untuk dapat melihat *username* dan *password.* Kerentanan ini tidak ditemukan.

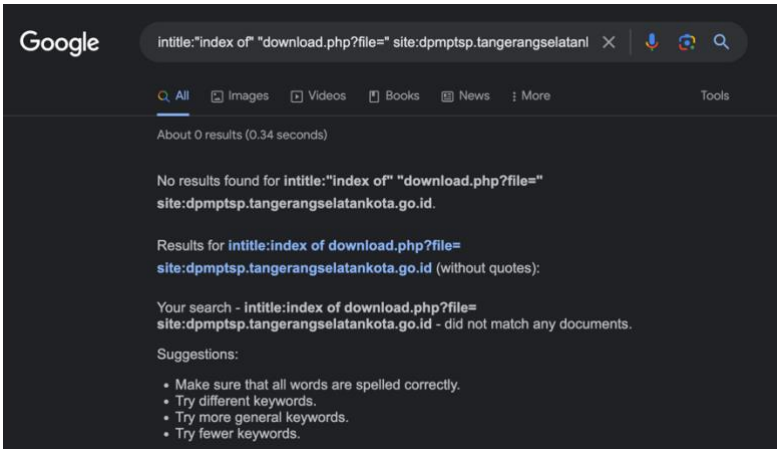
4. *Phpunit.yml*




Gambar 4. 12 Phpunit.yml

*Dork* yang diterbitkan pada 05-05-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan *database* yang tidak dilindungi. Kerentanan ini tidak ditemukan.

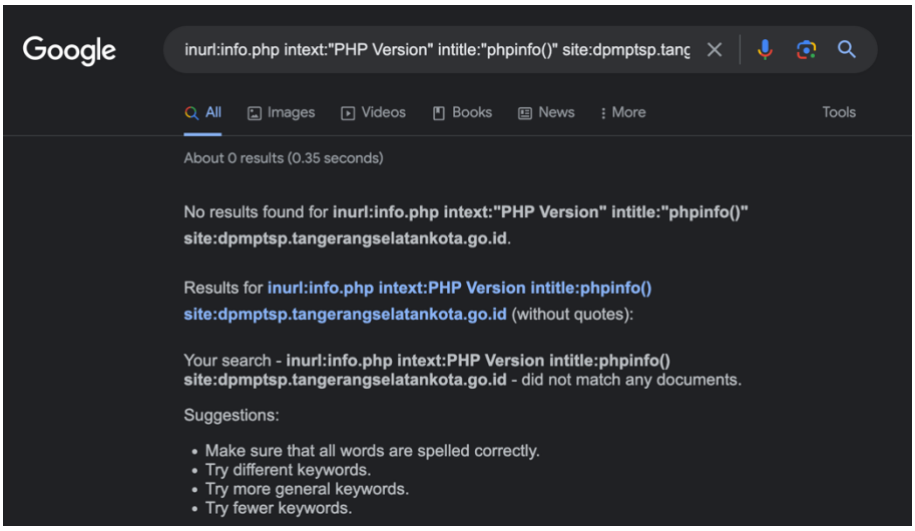
5. *Donwload.php?file=*




Gambar 4. 13 Download.php?file=

*Dork* yang diterbitkan pada 05-05-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan yang tidak dilindungi. Kerentanan ini tidak ditemukan.

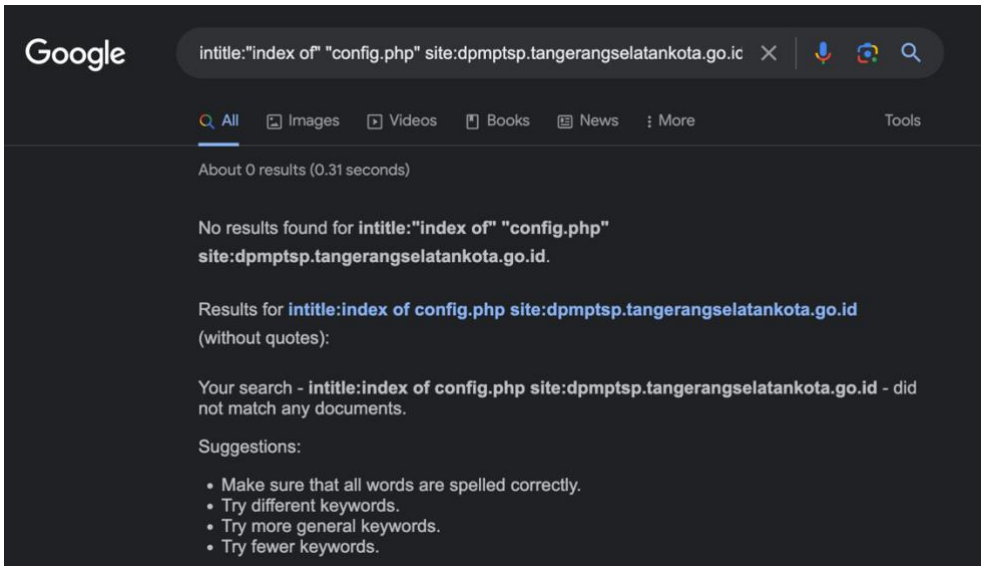
6. *Php Version*




Gambar 4. 14 Php Version

*Dork* yang diterbitkan pada 14-04-2023 ini merupakan suatu kerentanan yang menampilkan halaman informasi mengenai versi dari php yang digunakan. Kerentanan ini tidak ditemukan.

7. *Files containing juicy info*




Gambar 4. 15 Files containing juicy info

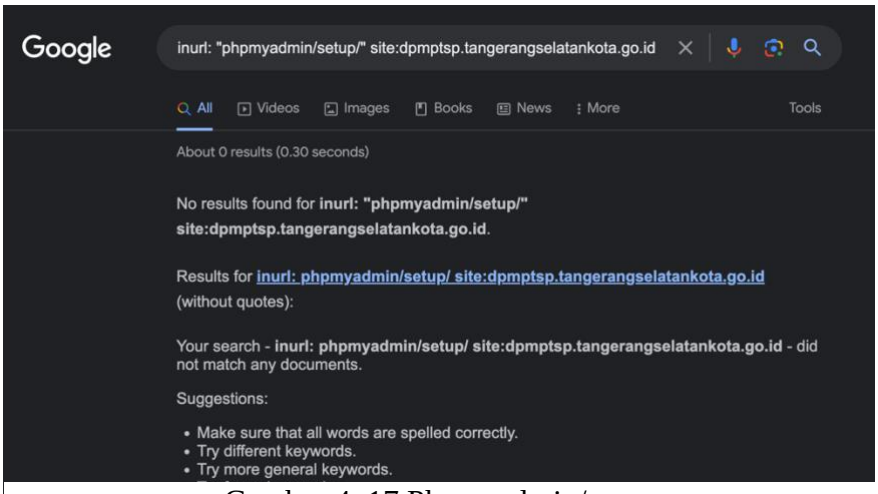
*Dork* yang diterbitkan pada 13-04-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan yang tidak dilindungi. Kerentanan ini tidak ditemukan.

8. *Admin/php*

Gambar 4. 16 Admin/php

*Dork* yang diterbitkan pada 21-03-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan *admin*. Kerentanan ini tidak ditemukan.

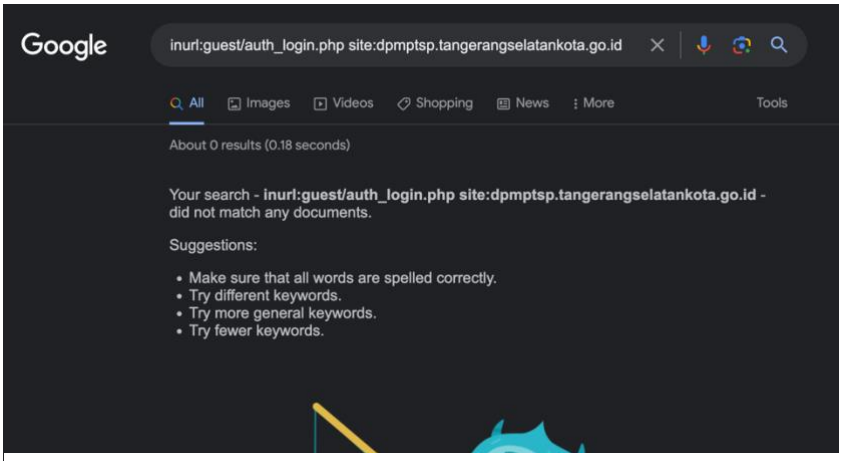
9. *Phpmyadmin/setup*




Gambar 4. 17 Phpmyadmin/setup

*Dork* yang diterbitkan pada 16-03-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan *phpMyAdmin/setup* seperti *config.php*, dan lain sebagainya. Kerentanan ini tidak ditemukan.

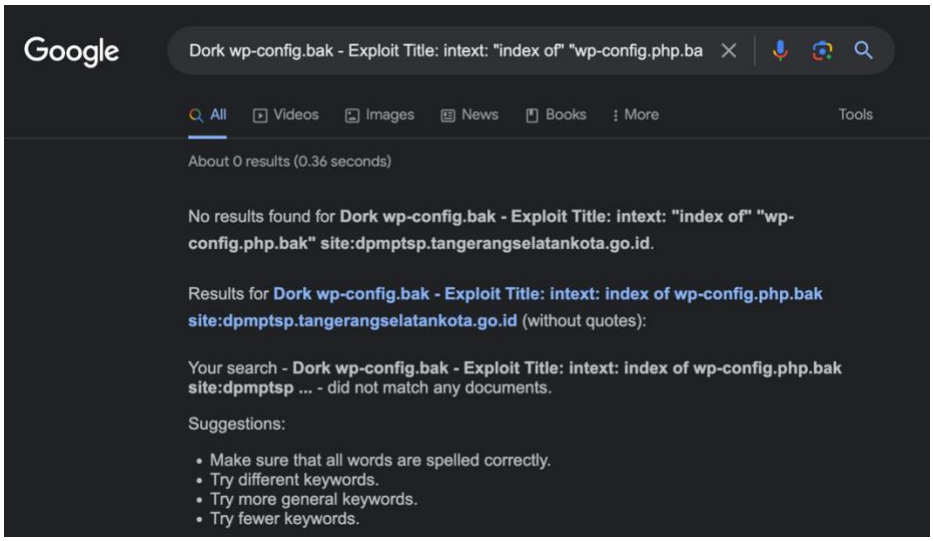
10. *Guest/auth_login.php*




Gambar 4. 18 Guest/auth_login.php

*Dork* yang diterbitkan pada 16-03-2023 ini merupakan suatu kerentanan yang membuat halaman *login* terekspoks. Kerentanan ini tidak ditemukan.

*11. Wp-config.php.bak*

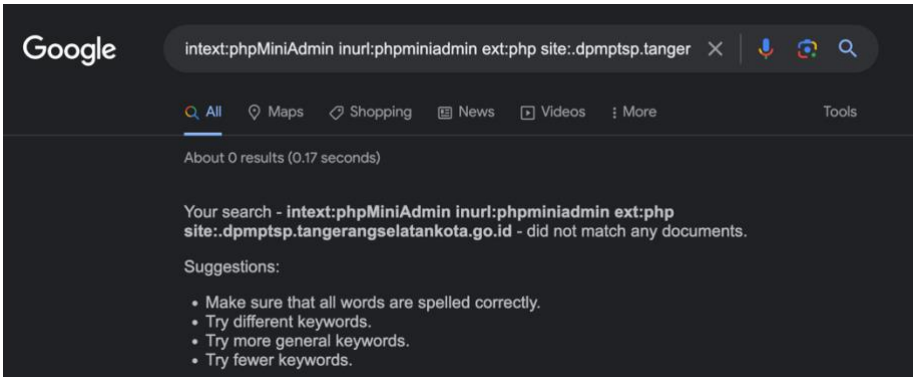



Gambar 4. 19 Wp-config.php.bak

*Dork* yang diterbitkan pada 27-02-2023 ini merupakan suatu kerentanan yang dapat mengakibatkan

munculnya informasi sensitif termasuk kredensial *database*. Kerentanan ini tidak ditemukan.

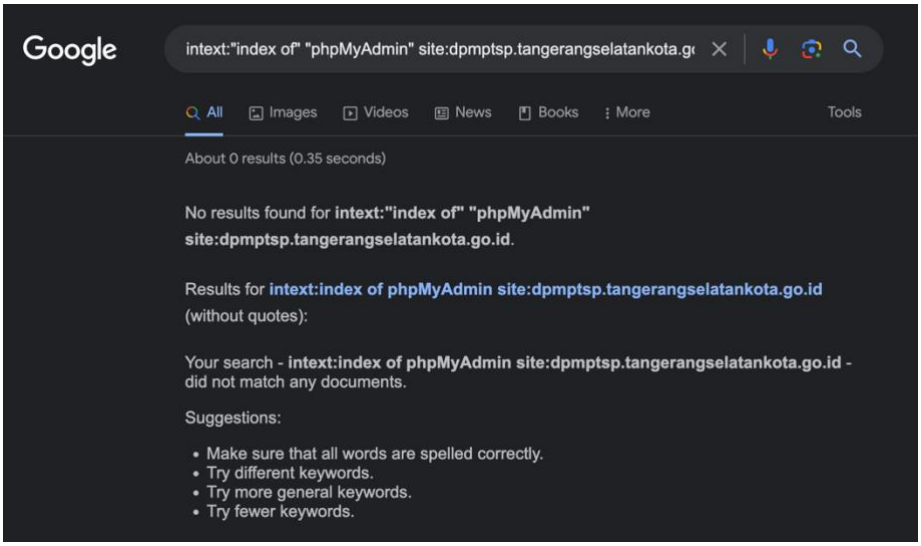
12. *phpMiniAdmin*




Gambar 4. 20 PhpMiniAdmin

*Dork* yang diterbitkan pada 22-02-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan yang tidak dilindungi. Kerentanan ini tidak ditemukan.

13. *PhpMyAdmin*

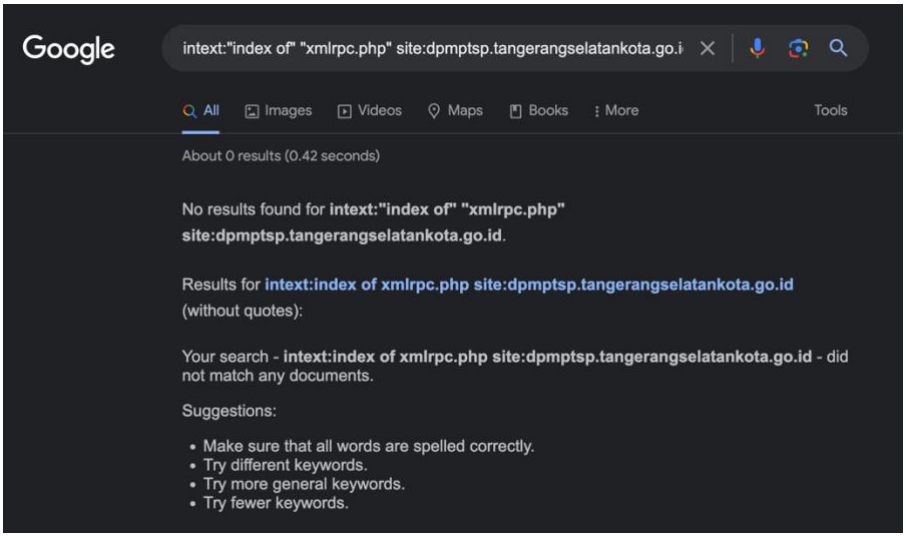



Gambar 4. 21 Index of PhpMyAdmin

*Dork* yang diterbitkan pada 07-02-2023 ini merupakan suatu kerentanan yang menampilkan halaman berisi file pengaturan didalam *phpMyAdmin* yang tidak dilindungi. Kerentanan ini tidak ditemukan.

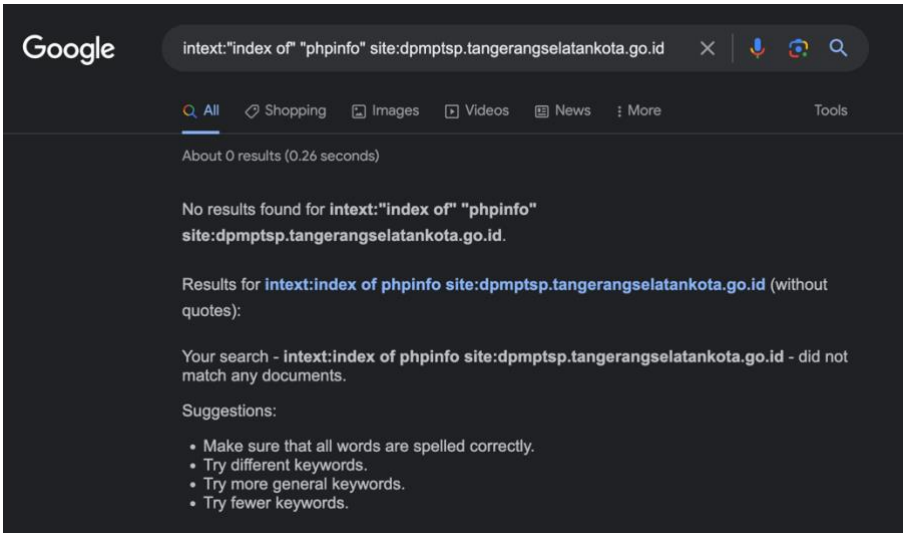
14. *Xmlrpc.php*

*Dork* yang diterbitkan pada 07-02-2023 ini merupakan suatu kerentanan yang dapat dimanfaatkan untuk mengumpulkan informasi *login*. Kerentanan ini tidak ditemukan.




Gambar 4. 23 Xmlrpc.php

15. *PhpInfo*




Gambar 4. 22 phpInfo

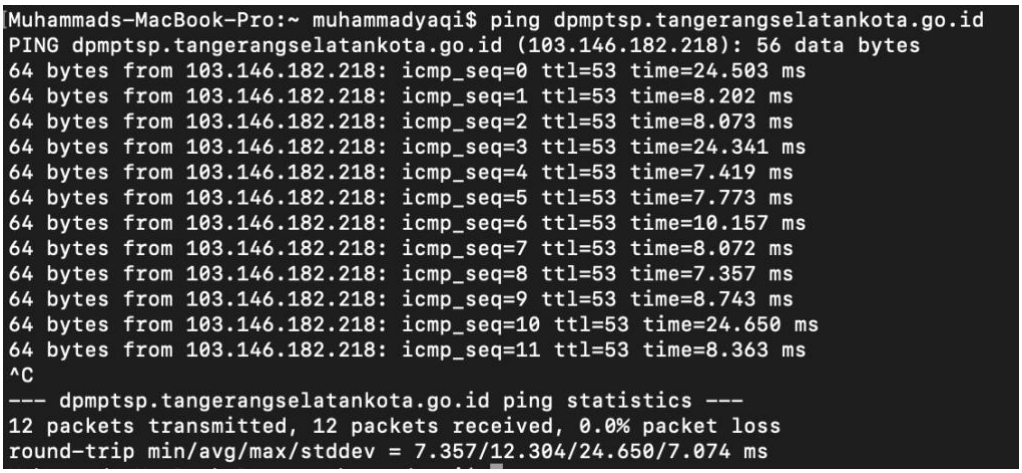
*Dork* yang diterbitkan pada 07-02-2023 ini merupakan suatu kerentanan yang menampilkan halaman

informasi mengenai versi dari php yang digunakan. Kerentanan ini tidak ditemukan.

### 4.2.2 Tahap *Scanning* (Pemindaian)

#### 4.2.2.1 *Ping*

Perintah *ping* dilakukan untuk mengetahui apakah *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan terkoneksi dengan jaringan, sebagai berikut.



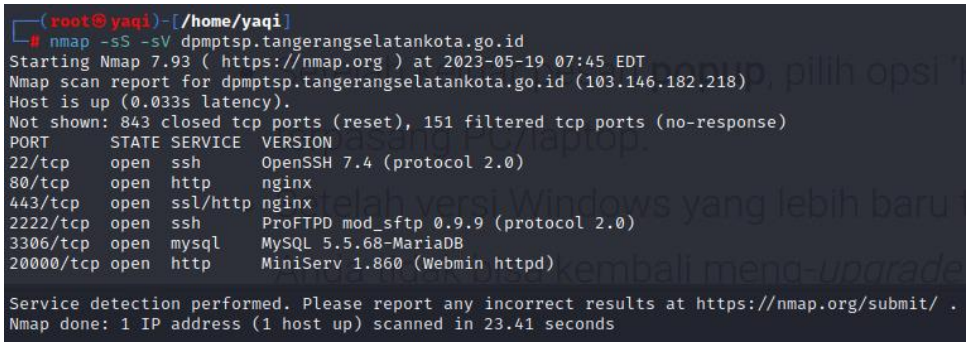

Gambar 4. 24 Hasil Ping

Pengiriman paket sebesar 64 *bytes* sebanyak 12 paket sukses diterima 100% dengan durasi minimal 7,357ms, dan maksimum 24,650ms dengan rata-rata 12,304ms.

#### 4.2.2.2 *Port Scanning* dengan *Nmap*

Dalam proses pemindaian pada *port* atau *port scanning*, Nmap versi 7.93 digunakan dengan beberapa perintah sebagai berikut.

1. *TCP Scan*



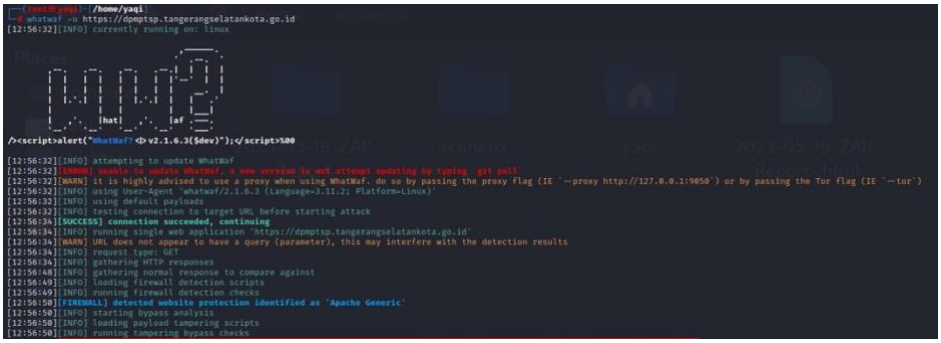

Gambar 4. 25 Hasil TCP Scan

Perintah -sS -sV [domain] digunakan untuk mendapatkan informasi mengenai *port* beserta versi yang digunakan, dengan keterangan lainnya terdapat sebanyak 843 *port* dalam keadaan tertutup dan 151 *port* tidak dapat ditentukan statusnya, atau dilindungi oleh *firewall*.

**Tabel 4. 4** Hasil Port Scanning Nmap

| *Port* | Status | Layanan | Versi |
|---|---|---|---|
| 22 | *Open* | SSH | *OpenSSH 7.4 (protocol 2.0)* |
| 80 | *Open* | HTTP | *Nginx* |
| 443 | *Open* | SSL/HTTP | *Nginx* |
| 2222 | *Open* | SSH | *ProFTD mod_sftp 0.9.9 (protocol 2.0)* |
| 3306 | *Open* | MYSQL | *MySQL 5.5.68-MariaDB* |
| 20000 | *Open* | HTTP | *MiniServ 1.860 (Webmin httpd)* |

Pengecekan terhadap *firewall* juga penulis lakukan dengan menggunakan *perintah 'whatwaf -u* [*domain*], sebagai berikut.




Gambar 4. 26 Hasil WhatWaf

Berdasarkan perintah ini, diketahui bahwa *firewall* yang digunakan oleh *website* ini adalah *Apache Generic*.

### 4.2.2.3 OWASP ZAP

Vulnerability Scanning akan dilakukan dengan menggunakan tools OWASP ZAP dengan memasukan alamat https://dpmptsp.tangerangselatankota.go.id, dengan hasil sebagai berikut.

| | | Confidence | | | | |
|---|---|---|---|---|---|---|
| | | User Confirmed | High | Medium | Low | Total |
| Risk | High | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) | 0 (0.0%) |
| | Medium | 0 (0.0%) | 1 (8.3%) | 1 (8.3%) | 0 (0.0%) | 2 (16.7%) |
| | Low | 0 (0.0%) | 1 (8.3%) | 5 (41.7%) | 1 (8.3%) | 7 (58.3%) |
| | Informational | 0 (0.0%) | 0 (0.0%) | 1 (8.3%) | 2 (16.7%) | 3 (25.0%) |
| | Total | 0 (0.0%) | 2 (16.7%) | 7 (58.3%) | 3 (25.0%) | 12 (100%) |

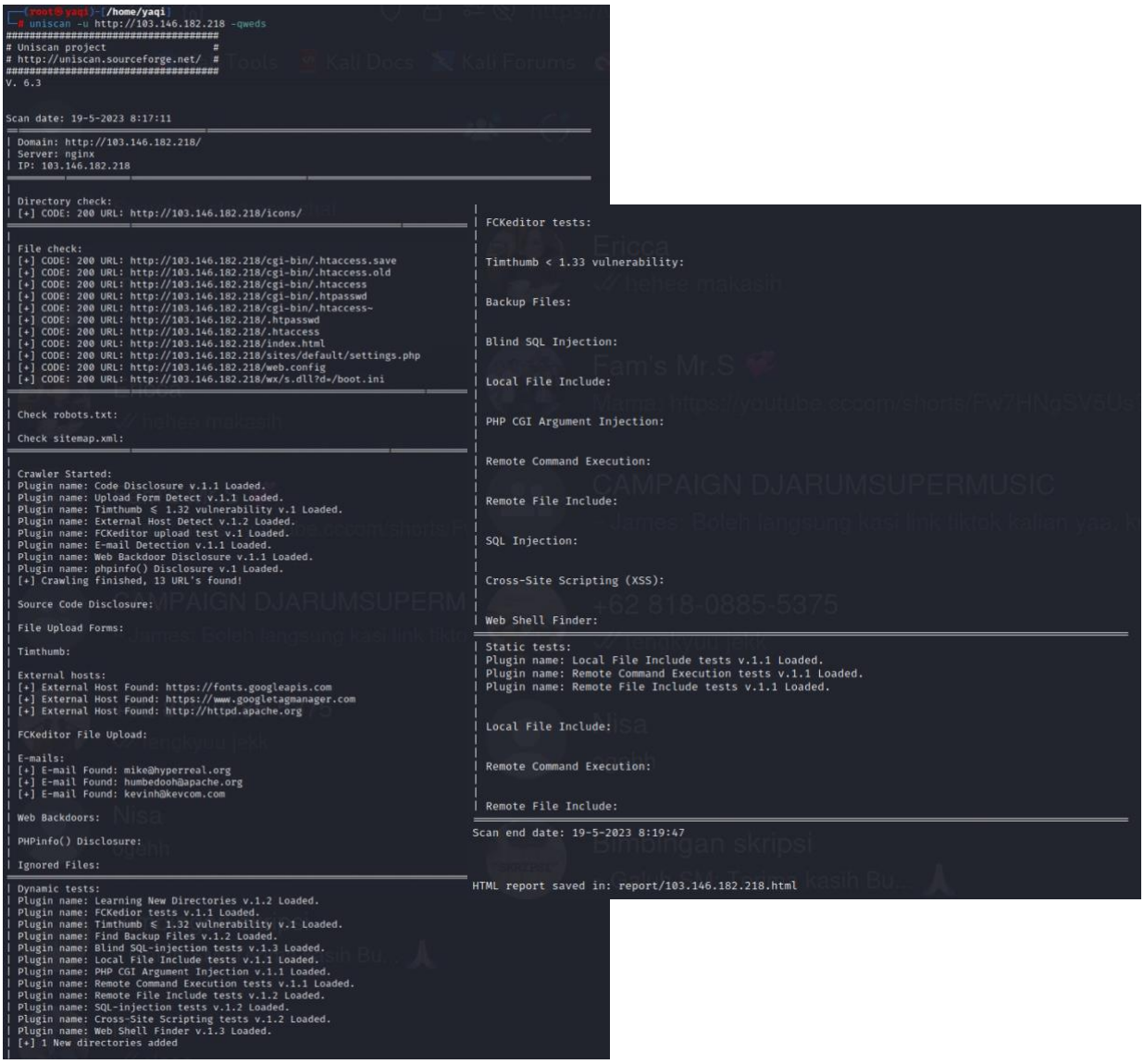
Gambar 4. 27 Hasil Scanning OWASP ZAP

Hasil kerentanan yang didapatkan akan dijelaskan sebagai berikut.

**Tabel 4. 5** Hasil Vulnerability Scanning dengan OWASP ZAP

| No. | Kerentanan | Tingkat Ancaman |
|---|---|---|
| 1 | *Content Security Policy* (CSP) *Header Not Set* | *Medium* |
| 2 | *Missing Anti-clickjacking Header* | *Medium* |
| 3 | *Cookie No HttpOnly Flag* | *Low* |
| 4 | *Cookie Without Secure Flag* | *Low* |
| 5 | *Cross-Domain javaScript Source File Inclusion* | *Low* |
| 6 | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | *Low* |
| 7 | *Strict-Transport-Security Header Not Set* | *Low* |
| 8 | *Timestamp Disclosure - Unix* | *Low* |
| 9 | *X-Content-Type-Options Header Missing* | *Low* |

#### 4.2.2.4 Uniscan

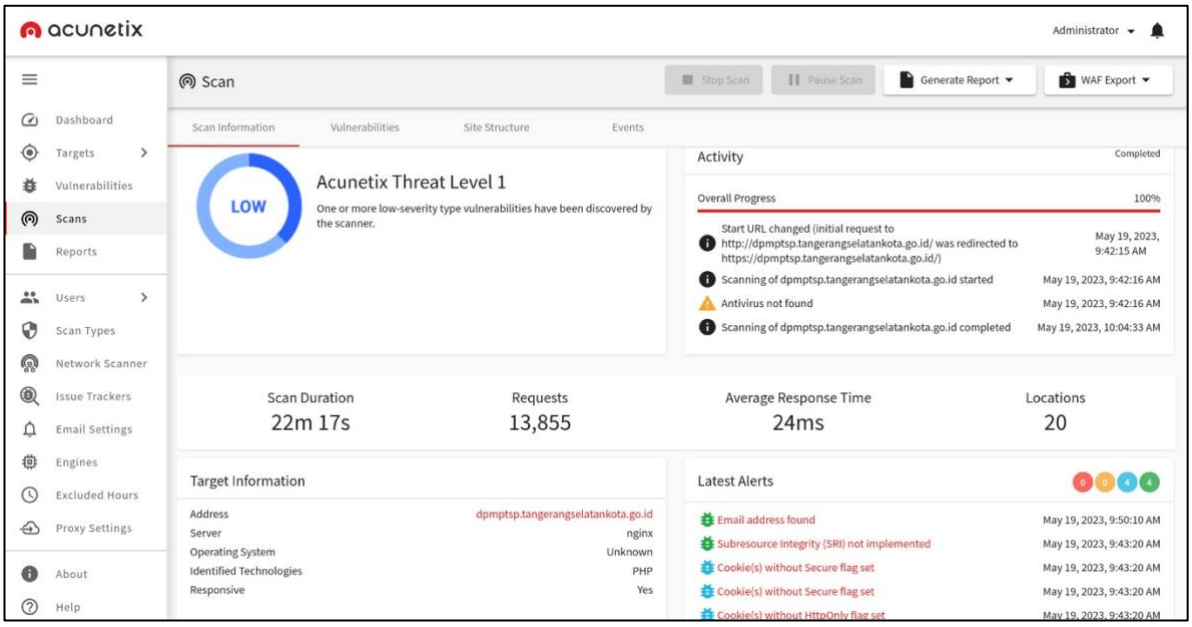



Gambar 4. 28 Hasil Uniscan

Berdasarkan hasil *vulnerability scanning* dengan *Uniscan*, diketahui terdapat informasi terkait *directory* dan *files*, tidak ditemukan robots.txt, terdapat beberapa *plugins* yang digunakan, 3 buah *email*, dan 3 *external host*, serta tidak ditemukan kerentanan seperti, *SQL Injection*, *Cross-Site Scripting* (XSS), dan lain sebagainya.

#### 4.2.2.5 Acunetix

Hasil *Vulnerability Scanning* yang dilakukan dengan




Gambar 4. 29 Hasil Scanning dengan Acunetix

menggunakan *Acunetix* dengan waktu pemindaian selama 22 menit 17 detik, dengan *request* sebanyak 13,855, dengan hasil sebagai berikut.

**Tabel 4. 6** Hasil Vulnerability Scanning dengan Acunetix

| No. | Kerentanan | Tingkat Ancaman |
|---|---|---|
| 1 | *Clickjacking: X-Frame-Options header missing* | *Low* |
| 2 | *Cookie(s) without HttpOnly flag set* | *Low* |
| 3 | *Cookie (s) without Secure flag set* | *Low* |

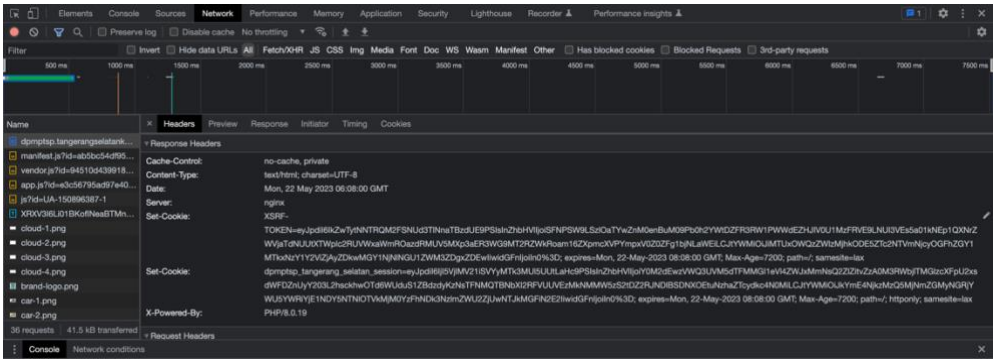
### 4.2.3 Tahap Eksploitasi (*Exploitation*)

Pada tahap ini akan dilakukan pengujian terkait celah kerentanan yang ditemukan pada tahapan sebelumnya dengan

menggabungkan hasil dari pemindaian kerentanan dengan OWASP ZAP dan Acunetix.

#### 4.2.3.1 *Content Security Policy* (CSP) *Header Not Set*

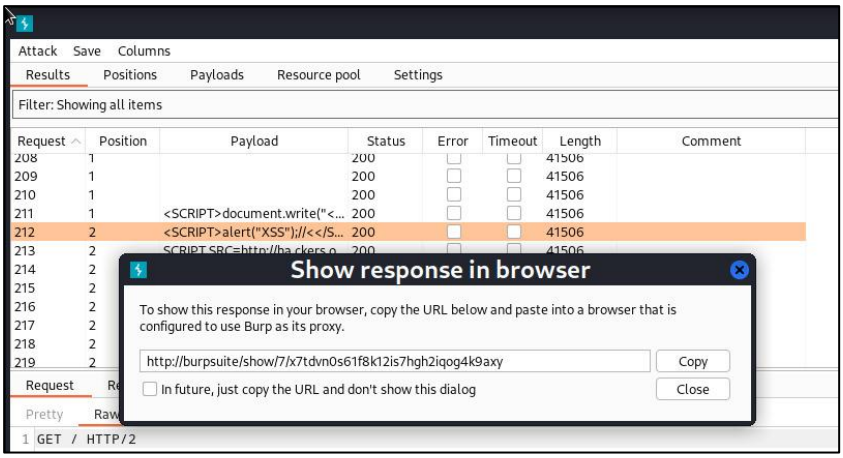
Kerentanan ini ditemukan berdasarkan hasil pemindaian dengan OWASP ZAP dengan tingkat kerentanan medium yang dapat menyebabkan adanya kemungkinan terkena serangan *Cross Site Scripting* (XSS) dan serangan *Injections*. Kerentanan ini tervalidasi melalui pengecekan melalui fungsi *inspect element* pada *browser*, bahwa *Content Security Policy (CSP) Header Not Set.*




Gambar 4. 30 Content Security Policy (CSP) Header Not Set

#### 4.2.3.2 *Cross Site Scripting (XSS)*

Tidak terpasangnya *Content Security Policy* (CSP) memungkinkan terjadinya serangan XSS yang akan diuji menggunakan *Burp Suite*, sebagai berikut.

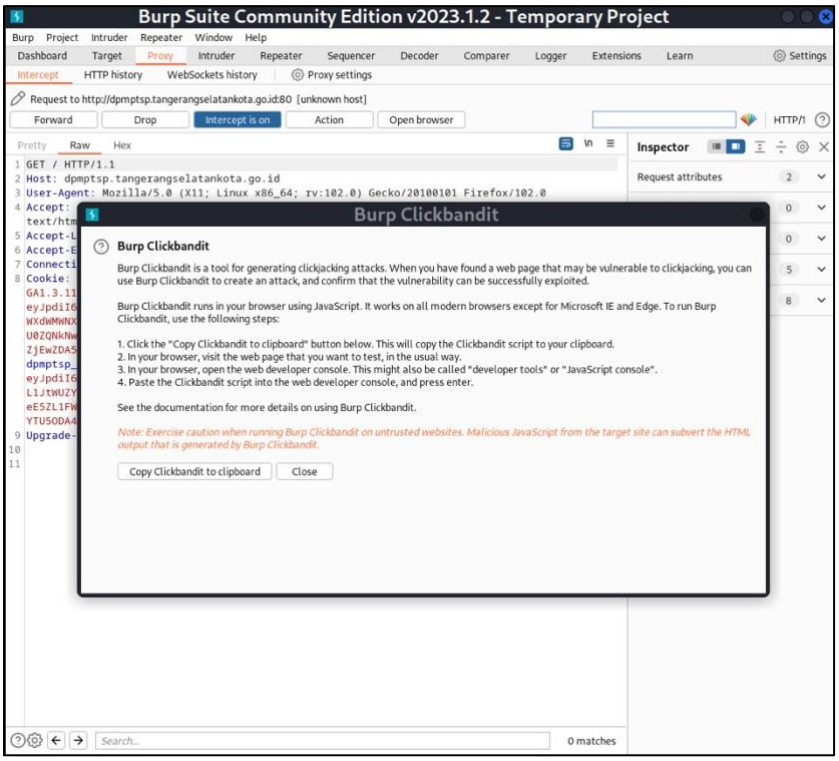



Gambar 4. 31 Cross Site Scripting (XSS)

Pengujian yang dilakukan dengan *Burp Suite* pada *Intruder Attack* dengan menggunakan *payloads* yang dalam hal ini digunakan yaitu ‘<SCRIPT>alert("XSS");//<</SCRIPT>’ dengan URL yang digunakan menjadi http://burpsuite/show/7/x7tdvn0s61f8k12is7hgh2iqog4k9axy, yang dinyatakan tidak berhasil dan mengembalikan perintah serangan ke halaman beranda *website* dpmptsp.tangerangselatankota.go.id.

#### 4.2.3.3 *Missing Anti-clickjacking Header*

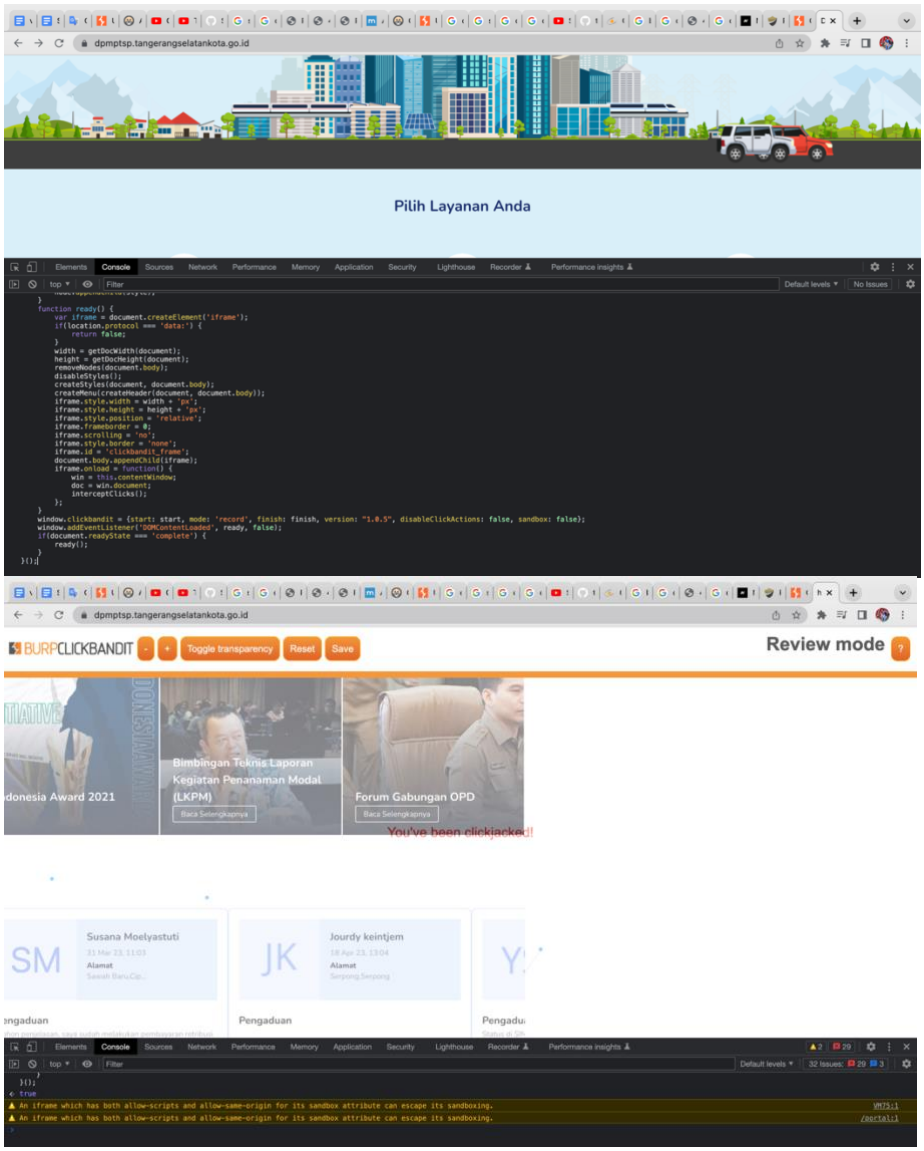
Penjelasan OWASP ZAP tentang kerentanan ini adalah sebagai sebuah respons tidak menyertakan Content-Security-Policy dengan arahan 'frame-ancestors' atau X-Frame-Options untuk melindungi dari serangan '*ClickJacking*'. Berdasarkan penjelasan ini, akan dilakukan *clickjacking attack* dengan menggunakan *Burp Suite*.




Gambar 4. 32 Burp Clickbandit

Tahap ini dilakukan dengan mengubah *intercept* menjadi *on* pada *Burp Suite*, kemudian melalui *browser* yang telah diatur *proxy* nya dengan HTTP *Proxy* 127.0.0.1 dengan *port* 8080, setelah di *intercept*, kemudian dapat memilih opsi *Burp Clickbandit* pada pada menu *Burp* untuk mendapatkan code yang akan digunakan sebagai *generating clickjacking attacks*.

Selanjutnya, pada halaman *website* masuk ke opsi *inspect element* dengan klik kanan pada *mouse*, kemudian click menu *console*, lalu *paste* dan *click enter* hingga memunculkan tampilan sebagai berikut.




Gambar 4. 33 Clickjacking Attacks

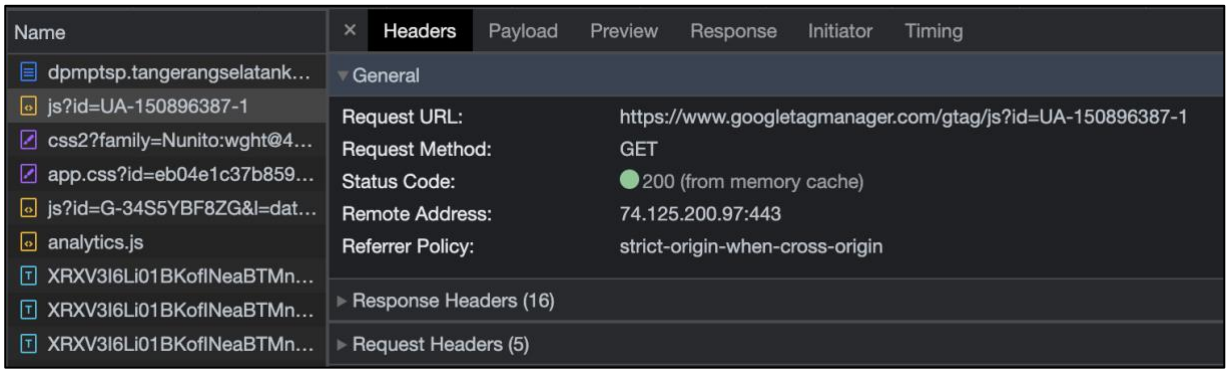
Eksploitasi ini akan dimulai dengan melakukan *click* pada *button* yang ada, kemudian finish. Kerentanan ini berhasil ditemukan dan tervalidasi dengan *clickjacking attacks* menggunakan *Burp Suite*.

#### 4.2.3.4 *Cookie No HttpOnly Flag & Cookie Without Secure Flag*

Gambar 4. 34 Cookie No HttpOnly Flag & Cookie Without Secure Flag

Cookie tanpa *HttpOnly* dan *secure flag* memungkinkan *cookie* dapat diakses oleh Javascript dan memungkinkan dapat diakses melalui koneksi yang tidak terenkripsi. Kerentanan ini ditemukan melalui *respons* yang didapatkan saat alamat yang telah di *intercept* dikirimkan ke *repeater* untuk kemudian di *send* dan mendapatkan *response*.

#### 4.2.3.5 *Cross Domain Javascript Source File Inclusion*




Gambar 4. 35 Informasi Javascript dari Domain Pihak Ketiga

Validasi terkait kerentanan ini dilakukan melalui fitur *inspect element* untuk melihat *response header* dari *Javascript* yang disediakan oleh domain pihak ketiga seperti pada Gambar 4.35. Kerentan ini berhasil ditemukan.

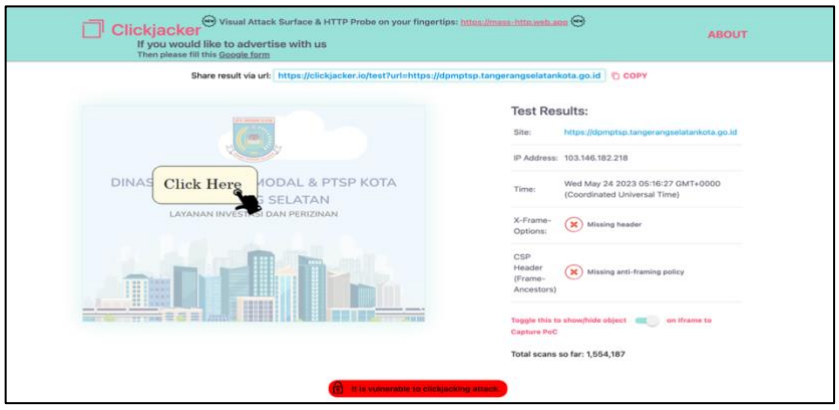
#### 4.2.3.6 *X-Content-Type-Options Header Missing*

*X-Content-Type-Options Header Missing* merupakan kerentanan dimana *server* tidak mengembalikan *X-Frame-Options* yang akan diuji menggunakan *Burp Suite* melalui fitur *repeater* dengan melakukan *GET request* sebagai

Gambar 4. 36 X-Content-Type-Options Header Missing

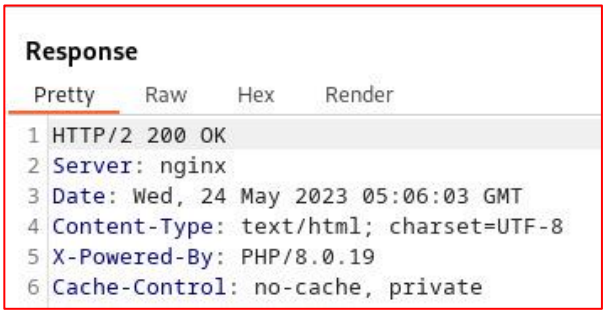
berikut.

*X-Content-Type-Options-Header* tidak ditemukan pada *response header*, kerentanan ini dapat menyebabkan serangan *clickjacking* yang akan diuji menggunakan *tools* online *clickjacker.io*, hal ini dilakukan untuk melakukan validasi dukungan karena sebelumnya telah dilakukan pengujian *clickjacking* menggunakan *Burp Suite.*




Gambar 4. 37 Clickjacking Check Menggunakan Clickjacker.io

#### 4.2.3.7 *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields*




Gambar 4. 38 X-Powered-By

Kerentanan ini berhasil ditemukan melalui *response* yang diberikan saat melakukan *GET request* pada fitur *repeater* di *Burp Suite* dengan indikasi bahwa *server* membocorkan informasi *X-Powered-By:PHP/8.0.19* yang dapat dimanfaatkan oleh penyerang untuk melakukan pencarian kerentanan yang mungkin ada pada komponen tersebut.

### 4.2.4 Tahap Post Exploitation

Tahap pasca eksploitasi dengan melakukan *backdoor* menggunakan *weevely* tidak dapat dilakukan, dikarenakan tidak adanya *field* untuk melakukan *upload file*, baik gambar ataupun *file* ekstensi lainnya. Sehingga, pasca eksploitasi yang dapat dilakukan adalah membuat laporan terkait tingkatan kerentanan yang ditemukan berdasarkan *Common Vulnerability Scoring System* (CVSS) pada tabel 4.7 sebagai berikut.

**Tabel 4. 7** Tabel Pengukuran Kerentanan dengan CVSS

| No | Kerentanan | Vektor String | Skor Kerentanan | |
|---|---|---|---|---|
| | | | Base Score | Peringkat Kualitatif |

| | | | | |
|---|---|---|---|---|
| 1 | *Missing Anti-clickjacking Header* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | 5.4 | *Medium* |
| 2 | *Conten Security Policy Header Not Set* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N | 4.7 | *Medium* |
| 3 | *X-Content-Type-Options Header Missing* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N | 4.3 | *Medium* |
| 4 | *Cross Domain Javascript Source File Inclusion* | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N | 3.7 | *Low* |
| 5 | *Cookie Without Secure Flag* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | 3.1 | *Low* |
| 6 | *Cookie No HttpOnly Flag* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | 3.1 | *Low* |
| 7 | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | 3.1 | *Low* |

**Tabel 4. 8** Summary Tahap Reconnaisance

| ***Tools*** | **Hasil** |
|---|---|
| *Whois* | IP: 103.146.182.218 |

| | |
|---|---|
| | ASN: AS137342 Diskominfo Tangerang Selatan |
| | Inetnum: 103.146.182.0 - 103.146.183.235 |
| | Netname: BTSNET-ID |
| | |
| *What Web* | *Web Server: Nginx* |
| | *Email: dpmptsp@tangerangselatankota.go.id* |
| | Javascript, HTML 5, PHP v8.0.19 |
| | |
| *The Harvester* | - |
| | |
| *CXSecurity* | *Nginx* 1.20.0 *Denial of Service* |
| | *Nginx* 1.20.0 *DNS Resolver Off-By-One Heap Write* |
| | |
| GHDB + *Google Dork* | - |
| | |

**Tabel 4. 9** Summary Tahap Scanning

| ***Tools*** | **Hasil** |
|---|---|
| *Ping* | 12 Paket sebesar 64*bytes* 100% diterima |
| | Durasi minimal 7,357ms |
| | Durasi maksimal 24,650ms |
| | Rata-rata 12,304ms |
| | |
| *Nmap* | *Port 22 \| Open \| SSH \| OpenSSH 7.4 (Protocol 2.0)\|* |
| | *Port 80 \| Open \| HTTP \| Nginx \|* |
| | *Port 443 \| Open \| SSL/HTTP \| Nginx \|* |
| | *Port 2222 \| Open \| SSH \| ProFTD mod_sftp 0.9.9 (protocol 2.0) \|* |
| | *Port 3306 \| Open \| MySQL \| MySQL 5.5.68-MariaDB \|* |
| | *Port 20000 \| Open \| HTTP \| MiniServ 1.860 (Webmin httpd) \|* |
| | |
| *What Waf* | WAF Apache Generic |
| | |
| *OWASP ZAP* | *Conten Security Policy* (CSP) *Header Not Set* |

| | |
|---|---|
| | *Missing Anti-clickjacking Header* |
| | *Cookie No HTTPOnly Flag* |
| | *Cookie Without Secure Flag* |
| | *Cross-Domain javaScript Source File Inclusion* |
| | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* |
| | *Strict-Transport-Security Header Not Set* |
| | *Timestamp Disclosure - Unix* |
| | *X-Content-Type-Options Header Missing* |
| | |
| *Uniscan* | Mengetahui *plugins* yang digunakan |
| | 3 Buah *e-mail* |
| | 3 *external host* |
| | |
| *Acunetix* | *Clickjacking: X-Frame-Options header missing* |
| | *Cookie(s) without HttpOnly flag set* |
| | *Cookie (s) without Secure flag set* |
| | |

**Tabel 4. 10** Summary Tahap Exploitation

| **Jenis Kerentanan** | **Hasil** |
|---|---|
| *Conten Security Policy* (CSP) *Header Not Set* | Berhasil ditemukan |
| | |
| *Cross Site Scripting* (XSS) | Tidak berhasil ditemukan |
| | |
| *Missing Anti-clickjacking header* | Berhasil ditemukan |
| | |
| *Cookie No HttpOnly Flag & Cookie Without Secure Flag* | Berhasil ditemukan |
| | |

| | |
|---|---|
| *Cross Domain Javascript Source File Inclusion* | Berhasil ditemukan |
| | |
| *X-Content-Type-Options Header Missing* | Berhasil ditemukan |
| | |
| *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | Berhasil ditemukan |
| | |

**Tabel 4. 11** Summary Tahap Post-Exploitation

| **Kegiatan** | **Hasil** | |
|---|---|---|
| *Backdoor* | Tidak dapat dilakukan, hal ini dikarenakan upaya *backdoor* berkaitan dengan mengupload file ke dalam sebuah *website*. Pada *website* ini tidak ditemukan *form* atau *field* untuk meng-*upload file backdoor* kedalam sistem | |
| | | |
| Pengukuran Kerentanan dengan *Common Vulnerability Scoring System* (CVSS) | *Missing Anti-clickjacking Header* | *Medium* |
| | *Conten Security Policy Header Not Set* | *Medium* |
| | *X-Content-Type-Options Header Missing* | *Medium* |
| | *Cross Domain Javascript Source File Inclusion* | *Low* |
| | *Cookie Without Secure Flag* | *Low* |
| | *Cookie No HttpOnly Flag* | *Low* |
| | *Server Leaks Information via* | *Low* |

| | | |
|---|---|---|
| | *'X-Powered-By' HTTP Response Header Fields* | |
| | | |

**Tabel 4. 12** Summary Tahap 1-4 Zero Entry Hacking (ZEH)

| **Reconnaisance** | | **Scanning** | | **Exploitation** | | **Post-Exploitation** | | |
|---|---|---|---|---|---|---|---|---|
| ***Tools*** | **Hasil** | ***Tools*** | **Hasil** | **Jenis Kerentanan** | **Hasil** | **Kegiatan** | **Hasil** | |
| *Whois* | IP: 103.146.182.218 | *Ping* | 12 Paket sebesar 64*bytes* 100% diterima | *Conten Security Policy* (CSP) *Header Not Set* | Berhasil ditemukan | *Backdoor* | Tidak dapat dilakukan, hal ini dikarenakan upaya *backdoor* berkaitan dengan mengupload file ke dalam sebuah *website*. Pada *website* ini tidak ditemukan *form* atau *field* untuk meng-*upload file backdoor* kedalam sistem | |
| | ASN: AS137342 Diskominfo Tangerang Selatan | | Durasi minimal 7,357ms | *Cross Site Scripting* (XSS) | Tidak berhasil ditemukan | Pengukuran Kerentanan dengan *Common Vulnerability Scoring System* (CVSS) | *Missing Anti-clickjacking Header* | *Medium* |
| | Inetnum: 103.146.182.0 - 103.146.183.235 | | Durasi maksimal 24,650ms | *Missing Anti-clickjacking header* | Berhasil ditemukan | | *Conten Security Policy Header Not Set* | *Medium* |
| | Netname: BTSNET-ID | | Rata-rata 12,304ms | *Cookie No HttpOnly Flag & Cookie Without Secure Flag* | Berhasil ditemukan | | *X-Content-Type-Options Header Missing* | *Medium* |
| *What Web* | *Web Server: Nginx* | *Nmap* | *Port 22 \| Open \| SSH \| OpenSSH 7.4 (Protocol 2.0)\|* | *Cross Domain Javascript Source File Inclusion* | Berhasil ditemukan | | *Cross Domain Javascript Source File Inclusion* | *Low* |
| | *Email: dpmptsp@tangerangselatankota.go.id* | | *Port 80 \| Open \| HTTP \| Nginx \|* | *X-Content-Type-Options Header Missing* | Berhasil ditemukan | | *Cookie Without Secure Flag* | *Low* |
| | Javascript, HTML 5, PHP v8.0.19 | | *Port 443 \| Open \| SSL/HTTP \| Nginx \|* | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | Berhasil ditemukan | | *Cookie No HttpOnly Flag* | *Low* |
| *The Harvester* | - | | *Port 2222 \| Open \| SSH \| ProFTD mod_sftp 0.9.9 (protocol 2.0) \|* | | | | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | *Low* |
| *CXSecurity* | *Nginx* 1.20.0 *Denial of Service* | | *Port 3306 \| Open \| MySQL \| MySQL 5.5.68-MariaDB \|* | | | | | |
| | *Nginx* 1.20.0 *DNS Resolver Off-By-One Heap Write* | | *Port 20000 \| Open \| HTTP \| MiniServ 1.860 (Webmin httpd) \|* | | | | |
| GHDB + *Google Dork* | - | *What Waf* | WAF Apache Generic | | | | | |
| | | *OWASP ZAP* | *Conten Security Policy* (CSP) *Header Not Set* | | | | | |
| | | | *Missing Anti-clickjacking Header* | | | | | |
| | | | *Cookie No HTTPOnly Flag* | | | | | |
| | | | *Cookie Without Secure Flag* | | | | | |
| | | | *Cross-Domain javaScript Source File Inclusion* | | | | | |
| | | | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | | | | | |
| | | | *Strict-Transport-Security Header Not Set* | | | | | |
| | | | *Timestamp Disclosure - Unix* | | | | | |
| | | | *X-Content-Type-Options Header Missing* | | | | | |
| | | *Uniscan* | Mengetahui *plugins* yang digunakan | | | | | |
| | | | 3 Buah *e-mail* | | | | | |

| | | | | |
|---|---|---|---|---|
| | | 3 *external host* | | |
| | *Acunetix* | *Clickjacking: X-Frame-Options header missing* | | |
| | | *Cookie(s) without HttpOnly flag set* | | |
| | | *Cookie (s) without Secure flag set* | | |

# BAB V
# HASIL DAN PEMBAHASAN

## 5.1 Hasil Identifikasi Kerentanan

Kerentanan yang telah didapatkan melalui tahapan *vulnerability scanning* dengan menggunakan *tools* OWASP ZAP, Nmap, dan Acunetix memberikan hasil yang tidak jauh berbeda. Di antara *tools* tersebut, OWASP ZAP mampu menghasilkan lebih banyak kerentanan yang terdeteksi pada target. Berdasarkan hal tersebut, kerentanan yang dimasukkan adalah kerentanan yang telah berhasil di uji dan diukur menggunakan kalkulator CVSS v3.1 sebagai berikut.

**Tabel 5. 1** Identifikasi Kerentanan

| No | Kerentanan | Peringkat | Dampak |
|---|---|---|---|
| 1 | *Missing Anti-clickjacking Header* | *Medium* | Dapat menyebabkan terserang oleh *clickjacking attack* |
| 2 | *Conten Security Policy Header Not Set* | *Medium* | Membuka kemungkinan yang lebih besar untuk terkena seranga *Cross Site Scripting* (XSS) |
| 3 | *X-Content-Type-Options Header Missing* | *Medium* | Memberikan kerentanan terhadap serangan *clickjacking* dan memungkin sebuah konten ditafsirkan sebagai sesuatu yang berbeda |
| 4 | *Cross Domain Javascript* | *Low* | Jika *file javascript* dari pihak ketiga yang diketahui secara sengaja atau tidak menyimpan *file* berbahaya, konten tersebut |

| | | | |
|---|---|---|---|
| | *Source File Inclusion* | | dapat ditambahankan atau dijalankan pada *website* terkait. |
| 5 | *Cookie Without Secure Flag* | *Low* | *Cookie* dapat diakses melalui koneksi atau jaringan yang tidak terenkripsi |
| 6 | *Cookie No HttpOnly Flag* | *Low* | *Cookie* dapat diakses oleh *javasript*, yang berarti akan berbahaya apabila yang ditampilkan adalah *cookie session* |
| 7 | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | *Low* | Dapat memfasilitasi *attacker* untuk mencari informasi mengenai komponen dari *website* yang ditampilkan |

## 5.2 Hasil Eksploitasi

### 5.2.1 *Cross Site Scripting* (XSS)

*Cross Site Scripting* (XSS) merupakan eksploitasi yang dilakukan dengan menempatkan injeksi pada sisi klien menggunakan halaman *website*. Pada pengujian kali ini, eksploitasi dilakukan karena ditemukan kerentanan *Content Security Policy Header Not Set* berdasarkan tabel 4.5 yang diketahui memiliki kemungkinan untuk terserang *Cross Site Scripting*. Meskipun tidak terdeksi, tapi penulis berusaha untuk mencari tau kemungkinan yang ada.

Pada pengujian ini, *payloads* yang digunakan pada *intruder attack* di *Burp Suite* mampu memberikan respon dengan status 200 yang artinya berhasil dikirim dan diterima, kemudian alamat dari *burp suite* di *copy* untuk kemudian dijalankan pada *proxy* 127.0.0.1 pada *port* 8080. Alamat ini tidak berhasil menampilkan *payloads* yang di *input*, lalu kemudian secara otomatis melakukan *redirect* ke alamat dpmptsp.tangeranselatankota.go.id.

### 5.2.2 *Clickjacking*

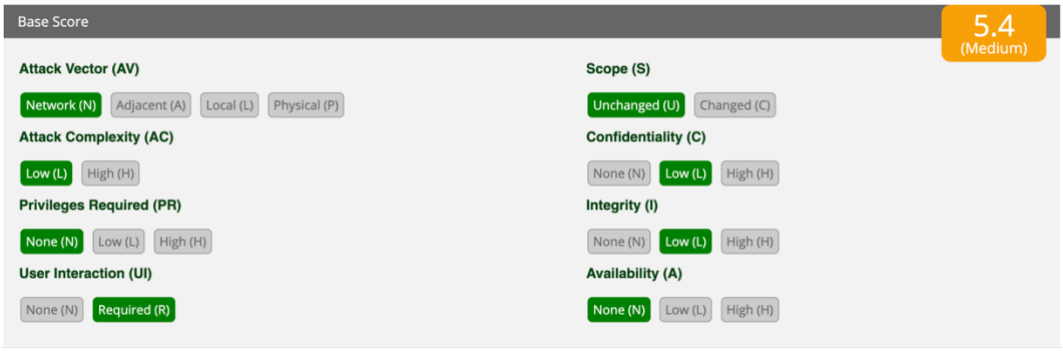
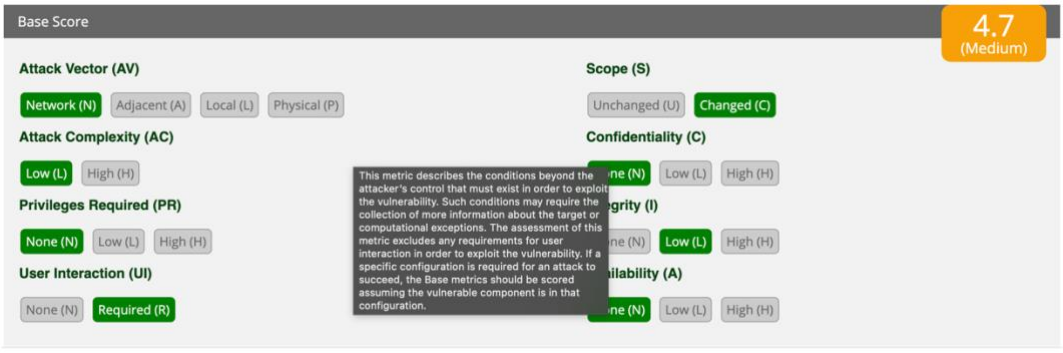
*Clickjacking* adalah serangan yang dilakukan dengan membajak *click button* yang tentunya tidak mudah disadari oleh kebanyakan pengguna. Serangan ini umumnya dilakukan untuk mengelabui pengguna agar melakukan *click* pada *button* yang dianggap benar, padahal itu adalah *button* tiruan dengan tujuan yang berbeda.

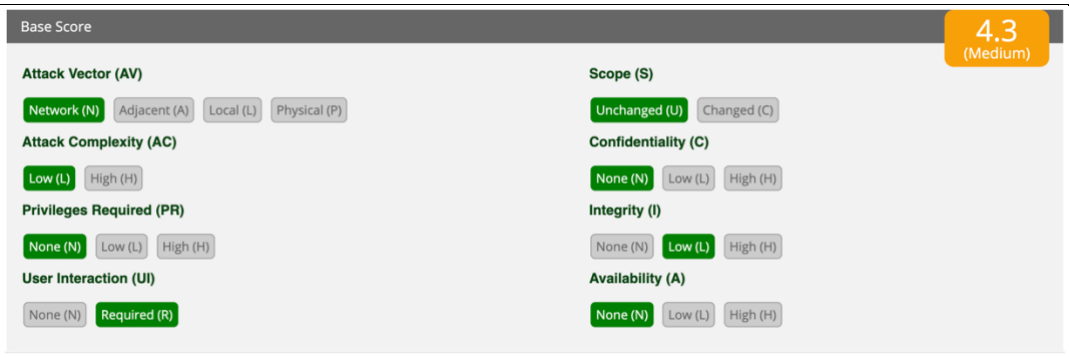
*Clickjacking* pada penelitian ini dilakukan dengan melakukan *intercept* alamat *website* target pada *Burp Suite* untuk kemudian memilih fitur *clickbandit* dan menyalin *code* didalamnya. Kemudian, halaman dpmptsp.tangerangselatankota.go.id dibuka dan di *inspect* kemudian *code* yang telah disalin di *paste* pada *tab console* kemudian tekan enter. Pengujian ini memvalidasi bahwa *website* dpmptsp.tangerangselatankota.go.id rentan terhadap *clickjacking attack* yang dapat dilihat pada gambar 4.33.

## 5.3 Pengukuran Kerentanan Menggunakan *Common Vulnerability Scoring System* (CVSS)

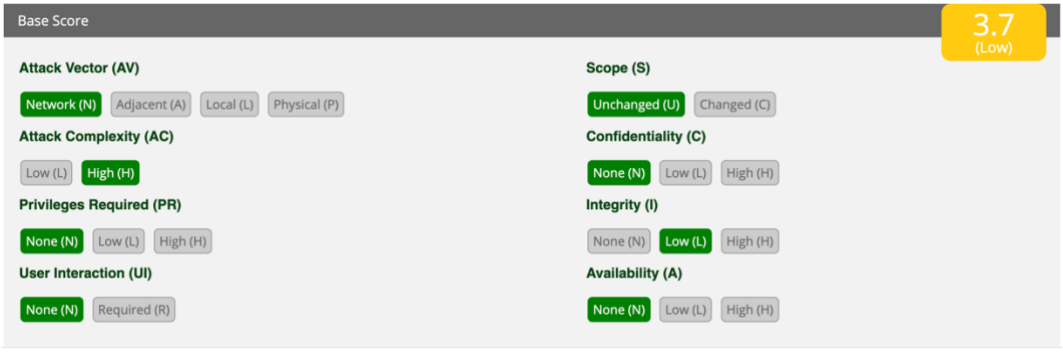
**Tabel 5. 2** Pengukuran Kerentanan dengan CVSS

| No | Kerentanan | Vektor String | Skor Kerentanan |
|---|---|---|---|

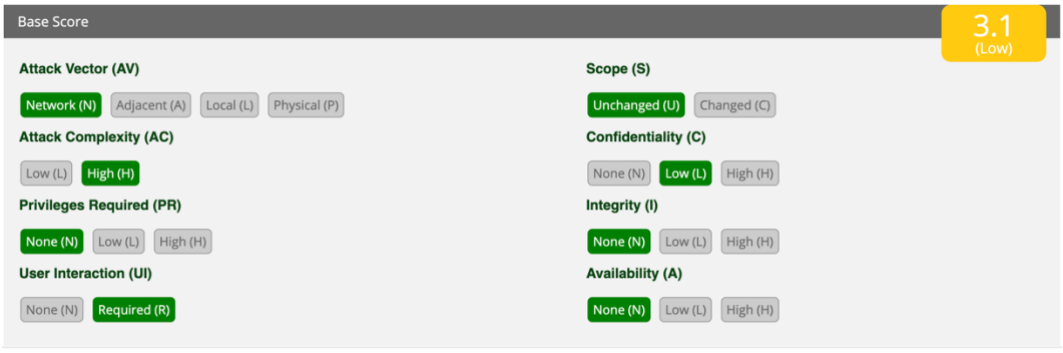
| | | | Base Score | Peringkat Kualitatif |
|---|---|---|---|---|
| 1 | *Missing Anti-clickjacking Header* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | 5.4 | *Medium* |
|  | | | | |
| 2 | *Conten Security Policy Header Not Set* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N | 4.7 | *Medium* |
|  | | | | |
| 3 | *X-Content-Type-Options Header Missing* | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N | 4.3 | *Medium* |



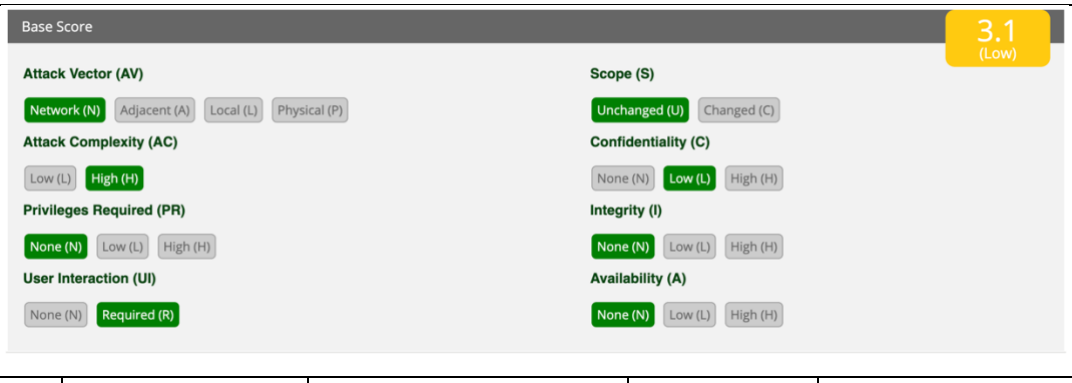

| | | | | |
|---|---|---|---|---|
| 4 | *Cross Domain Javascript Source File Inclusion* | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N | 3.7 | *Low* |



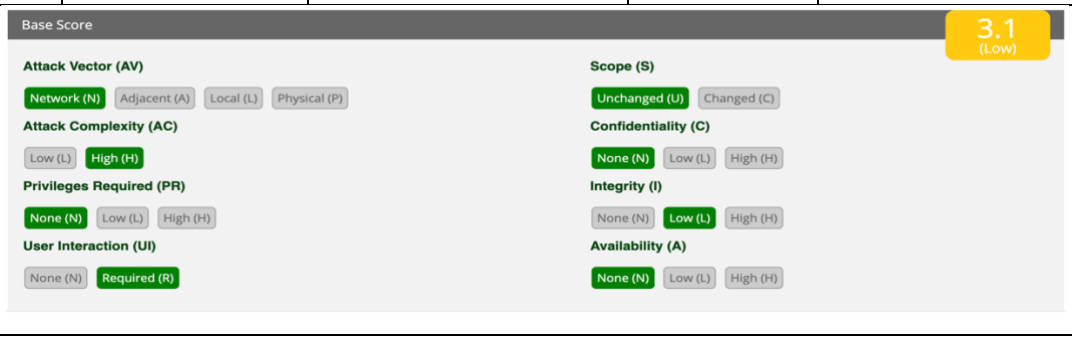

| | | | | |
|---|---|---|---|---|
| 5 | *Cookie Without Secure Flag* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | 3.1 | *Low* |




| | | | | |
|---|---|---|---|---|
| 6 | *Cookie No HttpOnly Flag* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | 3.1 | *Low* |




| | | | | |
|---|---|---|---|---|
| 7 | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | 3.1 | *Low* |




## 5.4 Rekomendasi Perbaikan

Rekomendasi perbaikan ini diberikan untuk membantu mengatasi masalah terkait celah kerentanan yang ditemukan. Adapun rekomendasinya berdasarkan OWASP sebagai berikut.

**Tabel 5. 3** Rekomendasi Perbaikan

| No | Kerentanan | Rekomendasi |
|---|---|---|
| 1 | *Missing Anti-clickjacking Header* | Pastikan *Conten Security Header Policy* dan *X-Frame-Options*, dapat juga untuk mempertimbangkan alternatif penerapan '*frame-ancestors*'. |

| | | |
|---|---|---|
| 2 | *Conten Security Policy Header Not Set* | Memastikan ulang bahwa *web server*, *application server*, *load balancer*, dan lain sebagainya telah terpasang *Conten Security Header Policy* dengan baik. |
| 3 | *X-Content-Type-Options Header Missing* | Pastikan bahwa aplikasi atau *web server* menyetel *Content-Type* dengan benar, dan menyetel *X-Content-Type-Options* ke 'nosniff' untuk semua halaman web. Pastikan bahwa pengguna akhir menggunakan browser web yang sesuai standar dan modern yang tidak melakukan pelacakan MIME sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan pelacakan MIME. |
| 4 | *Cross Domain Javascript Source File Inclusion* | Pastikan *file* sumber *JavaScript* dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi. |
| 5 | *Cookie Without Secure Flag* | Setiap kali *cookie* berisi informasi sensitif atau merupakan token sesi, *cookie* harus selalu diteruskan menggunakan saluran terenkripsi. Pastikan bendera aman disetel untuk *cookie* yang berisi informasi sensitif tersebut. |
| 6 | *Cookie No HttpOnly Flag* | Pastikan bendera *HttpOnly* disetel untuk semua *cookie*. |

| | | |
|---|---|---|
| 7 | *Server Leaks Information via 'X-Powered-By' HTTP Response Header Fields* | Pastikan *web server*, *application server*, *load balancer*, dan lain sebagainya dikonfigurasi untuk menekan header "*X-Powered-By*". |

# BAB VI
# KESIMPULAN DAN SARAN

## 6.1 Kesimpulan

Dalam melakukan implementasi *Vulnerability Assessment* dan *Penetration Testing* (VAPT) yang bertujuan untuk melakukan pemindaian dan pengujian keamanan pada sebuah *web* berdomain dpmptsp.tangerangselatankota.go.id milik Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan yang telah dilakukan oleh penulis, dapat disimpulkan sebagai berikut:

1. Melalui tahapan pada metode *Zero Entry Hacking* (ZEH) berhasil ditemukan celah kerentanan yang pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan antara lain, *missing anti-clickjacking header*, *content security policy (csp) header not set*, *x-content-type-options header missing*, *cross domain javascript source file inclusion*, *cookie without secure flag*, *cookie without Httponly flag*, *server leaks information via 'x-powered-by' HTTP response header fields.*
2. Kondisi keamanan pada *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dapat dikatakan sudah cukup baik mengacu pada hasil pengukuran kerentanan dengan CVSS yang menghasilkan tiga kerentanan dengan tingkat *medium*, dan empat kerentanan berada pada tingkat *low*, tanpa ditemukannya celah kerentanan dengan tingkatan *high*.

## 6.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk penelitian selanjutnya, khususnya bagi kemanan *website* Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan sebagai objek penelitian dalam penelitian ini yang antara lain:

1. Bagi Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan

- Perlu dilakukan *maintenance* sistem secara berkala pada *website* dpmptsp.tangerangselatankota.go.id untuk mengetahui celah sejak awal sehingga dapat meminimalisir adanya serangan dan dapat dilakukan perbaikan.
- Melakukan perbaikan khususnya pada *security header* untuk meminimalisir kemungkinan buruk dari meluasnya celah kerentanan yang mungkin dapat ditimbulkan.
- Segera melakukan perbaikan berdasarkan hasil rekomendasi penelitian yang telah dilakukan pada penelitian ini, berdasarkan tingkat kerentanan yang diukur menggunakan kalkulator *Common Vulnerability Scoring System v3.1*.

2. Bagi Penelitian Selanjutnya
    - Menggunakan pengujian keamanan dengan metode *White-box testing* atau *Black-box Testing.*
    - Melakukan pengujian dengan cara *social engineering*.
    - Melakukan perhitungan skor kerentanan menggunakan *tools* lain seperti *Common Weakness Enumeration* (CWE) dan *Common Vulnerabilities and Exposures* (CVE).

# DAFTAR PUSTAKA

Abas, W. (2013). Analisa Kepuasan Mahasiswa Terhadap Website Universitas Negeri Yogyakarta (Uny). *Manajemen*, 1–6.

Adani, M. R. (2020). *Jaringan Komputer: Pengertian, Jenis, Topologi dan Manfaat*. Sekawan Media.

Agustina, D., Pramadista, F. N., & Regyna, T. F. (2015). Sistem Manajemen Keamanan Informasi. *Syria Studies*, *7*(1), 37–72. https://www.researchgate.net/publication/269107473_What_is_governance/link/548173090cf22525dcb61443/download%0Ahttp://www.econ.upf.edu/~reynal/Civil wars_12December2010.pdf%0Ahttps://think-asia.org/handle/11540/8282%0Ahttps://www.jstor.org/stable/41857625

Aini, Q., Shofi, I. M., & Agustin, F. E. M. (2019). Analisis Website Perpustakaan Universitas Islam Negeri Menggunakan Metode Benchmarking Dan Goal Oriented Requirments Engineering (Gore) Model (Studi Kasus: Uin Jakarta, Uin Yogyakarta Dan Uin Malang). *Jurnal Teknik Informatika*, *12*(2), 159–166. https://doi.org/10.15408/jti.v12i2.13245

Al Fajar, F. (2020). Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability. *Inova-Tif*, *3*(2), 110. https://doi.org/10.32832/inova-tif.v3i2.4127

Aliefyan, A. (2020). Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web. *ResearchGate*, *July*.

Anas, M. A., Soepriyanto, Y., & Susilaningsih. (2018). Pengembangan Multimedia Tutorial Topologi Jaringan Untuk SMK Kelas X Teknik Komputer dan Jaringan. *Jurnal Kajian Teknologi Pendidikan*, *1*(4). http://journal2.um.ac.id/index.php/jktp/article/view/6916/3859

Andria, , Wahyu Ambar Ningrum, & Mubarok, I. (2021). Pengujian keamanan basis data sistem informasi berbasis web. *Seminar Nasional Aplikasi Sains & Teknologi (SNAST), Prosiding SNAST 2021*, 66–74.

Arafat, A. A. (2020). Penetration Testing Pada Website Registrar Pengelola Nama Domain Internet Indonesia ( Pandi ). In *UIN Syarif Hidayatullah Jakarta* (Vol. 20).

Asrin, A. (2022). Metode Penelitian Eksperimen. *Maqasiduna: Journal of Education, Humanities, and Social Sciences*, *2*(01), 21–29. https://doi.org/10.59174/mqs.v2i01.24

Astuti, I. K. (2018). *Jaringan Komputer*. 8. https://id.scribd.com/document/503304719/jaringan-komputer

Aziz, A., & Tampati, T. (2015). Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx. *Multinetics*, *1*(2), 12. https://doi.org/10.32722/multinetics.vol1.no.2.2015.pp.12-20

Azizah, R. Z. H. (2020). Mendefinisikan Kembali Konsep Keamanan dalam Agenda Kebijakan Negara-Bangsa Redefining the Concept of Security in the Nation-State Policy Agenda. *Diplomasi Pertahanan*, *6*(September 2001), 94–104.

Badan Pusat Statistik. (2022). *Indeks Pembangunan Teknologi Informasi Informasi dan Komunikasi 2021* (Vol. 13, Issue 1). Badan Pusat Statistik.

Bayu Rendro, D., & Nugroho Aji, W. (2020). Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang). *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115. https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/2522

Božić, K., Penevski, N., & Adamović, S. (2019). *Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods*. *January*, 229–234. https://doi.org/10.15308/sinteza-2019-229-234

Bride, M. (2003). *Internet* (1st ed.). Kesaint Blanc.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Chandra, A. N., Sylviana, F., & Nugrahaningsih, N. (2021). Website Pemesanan Penginapan Di Palangka Raya. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *15*(1), 34–43. https://doi.org/10.47111/jti.v15i1.1935

Chazar, C. (2017). Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005. *Jurnal Informasi*, *VII*(2), 48–57.

Cloudmatika. (2022). *Mengenal 6 Jenis-jenis Web Server bagi Website Anda*. Cloudmatika.

Coding Studio Team. (2021). *Mengenal Network Penetration Testing dan Cara Kerjanya*.

Cole, E. (2005). *Network Security Bible*. Wiley Publishing.

CXSecurity. (2023). *CXSecurity Free Vulnerability Database*. CXSecurity. https://cxsecurity.com/wlb/about/

Cyber Academy Indonesia. (2022). *3 Jenis Hacker Yang Perlu Kamu Tahu*. Cyber Academy Indonesia.

Cybervie.com. (2022). *What is theHarvester?* https://www.cybervie.com/blog/what-is-the-harvester/

Direktorat Operasi Keamanan Siber. (2022). *Laporan bulanan publik (HASIL MONITORING KEAMANAN SIBER)*. *70*, 12. https://cloud.bssn.go.id/s/HoFJzyeFASPqawL

Dougpoer. (2015). *Uniscan*. https://sourceforge.net/projects/uniscan/

Dpmptsp. (2023). *DPMPTSP Tangerang Selatan*. Dpmptsp Kota Tangerang Selatan. https://dpmptsp.tangerangselatankota.go.id/tentang-kami

Dwiyankuntoko, A. (2013). Membandingkan Protokol UDP dan TCP. *Komunitas ELearning IlmuKomputer.Com*, 1–6.

DzulfIqar, M. D. (2017). Perancangan Website UIN Syarif Hidayatullah Jakarta Mengunakan Metode User Centered Design Dengan Standard ISO 9126. *Universitas Islam Negeri Syarif Hidayatullah*.

Engebretson, P. (2013). *The Basic of Hacking and Penetration Testing*. Elsevier Hadnagy.

Engebretson, P. H., Pauli, J. J., & Streff, K. F. (2008). An ethical network hacking

contest for undergraduate student recruitment. *Proceedings of the 2008 International Conference on Frontiers in Education: Computer Science and Computer Engineering, FECS 2008*, *January 2008*, 68–74.

Fathurrachman. (2023). *PENGUJIAN KERENTANAN LOG4SHELL PADA WEBSITE E-COMMERCE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT AND PENETRATION TESTING ( VAPT ) LIFE CYCLE PENGUJIAN KERENTANAN LOG4SHELL PADA WEBSITE E-COMMERCE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT AND PENETRATI*.

FIRST. (2019). *Common Vulnerability Scoring System version 3.1 Specification Document Revision 1*. 1–24. https://www.first.org/cvss/

Fortinet. (2023). *What is Web Security and Website Security?* Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-web-security#:~:text=is web security%3F-,Web security refers to protecting networks and computer systems from,they are designed to provide.

Gani, A. G. (2014). Pengenalan Teknologi Internet Serta Dampaknya. *Jurnal Sistem Informasi Universitas Suryadarma*, *2*(2). https://doi.org/10.35968/jsi.v2i2.49

Germanotta, J. (2021). *Metodologi dan Standar Penetration Testing*. https://biztech.proxsisgroup.com/top-5-metodologi-dan-standar-penetration-testing/

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

Hamim, N. (2021). *Cara Menggunakan Perintah Nmap di Linux*. Belajar Linux. https://belajarlinux.id/cara-menggunakan-nmap-di-linux/

Hasbullah, M. S. (2018). *Analisis Perbandingan Web Server Apache dan Nginx Menggunakan Apache Jmeter Pada Server Aplikasi Ais Yang Berbasis Clustering Server*.

Hayaty, N. (2020). *Buku Ajar: Sistem Keamanan*. 1–99.

Heartly, R. (2003). *Sistem Informasi Manajemen*. *2*.

http://bangdanu.wordpress.com

Hidayat, A. (2021). *Penelitian Eksperimen*. Statistikian. https://www.statistikian.com/2012/10/penelitian-experimen.html

Ichsani, Y. (2018). Evaluasi Performa Usability Situs-Situs Web Perguruan Tinggi Negeri Di Indonesia Yang Terakreditasi "a" Tahun 2013 Serta Perbandingan Kondisi Situs Web Tahun 2014 Dan 2017. *Jurnal Teknik Informatika*, *10*(2), 93–108. https://doi.org/10.15408/jti.v10i2.6824

Idfaris. (2020). *BackConnect menggunakan weevely3 di ubuntu*. Medium.Com. https://medium.com/@idfaris.official/backconnect-menggunakan-weevely3-di-ubuntu-73e1c435cbd5

Ilmu Bersama. (2021). *Hacking Lab – Setup Burp Suite di Kali Linux*. Ilmubersama.Com. https://ilmubersama.com/2021/02/22/hacking-lab-setup-burp-suite-di-kali-linux/

Irawan, I. (2022). *Implementasi Keamanan Jaringan Pada Cloudfri Dengan Metode Hardening*. *9*(2), 644–649.

Janner Simarmata, Dimas Sasongko, J. I. S., Yuswardi, Mimin Fatchiyatur Rohmah, S. A. H. U., Sitti Arni, Sugianto, Jamaludin, A. A., & Ilham Firman Ashari, Zelvi Gustiana, L. A. (2022). *Sistem keamanan data* (R. Watrianthos (ed.); Issue October).

Jiwandono, A. (2021). Analisa Perbandingan Kinerja Web Server Apache, Nginx, Dan Litespeed Dengan Menggunakan Metode Stress Test. *Diss. Universitas Islam Riau*.

kali.org. (n.d.). *Weevely*. Kali.Org. Retrieved March 31, 2023, from https://www.kali.org/tools/weevely/

kali.org. (2022). *Whatweb*. https://www.kali.org/tools/whatweb/

kali.org. (2023). *Burp Suite*. Kali.Org. https://www.kali.org/tools/burpsuite/

Kaurvaki, R. (2023). *Mengenal Secara Lengkap Apa itu Whois Domain dan Whois Privacy*. Pandagila.Com. https://pandagila.com/whois-domain-privacy/

Kbbi. (n.d.). *Aman*. https://kbbi.web.id/aman

Khan, M. E., & Khan, F. (2012). A Comparative Study of White Box, Black Box and Grey Box Testing Techniques. *International Journal of Advanced*

*Computer Science and Applications*, *3*(6), 12–15. http://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203

Khera, Y., Kumar, D., Sujay, S., & Garg, N. (2019). Analysis and Impact of Vulnerability Assessment and Penetration Testing. *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019, February 2019*, 525–530. https://doi.org/10.1109/COMITCon.2019.8862224

Klusaite, L. (2020). *Perbedaan UDP dan TCP*. NordVPN.

Kusnanto, Y. (2016). Analisis Kerentanan Dan Kehandalan Layanan Jaringan Cloud Berbasis Platform Eucalyptus. *Jurnal Sistem Informasi (JSI)*, *8*(1), 2355–4614. http://ejournal.unsri.ac.id/index.php/jsi/index

Kusnendi, M. S., & Modul, M. S. (2017). Konsep Dasar Sistem Informasi. *Konsep Dasar Sistem Informasi*, 1–36.

Kusuma, G. (2022). Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik. *Jurnal Teknologi Informasi: Jurnal Keilmuan Dan Aplikasi Bidang Teknik Informatika*, *16*(2), 178–186. https://doi.org/10.47111/jti.v16i2.3995

Listartha, I. M. E., Saskara, G. A. J., & Santyadiputra, G. S. (2021). *KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications*. *4*(2), 1–14.

Loshin, P. (2022). *Application Security*. Senior Technology Editor. https://www.techtarget.com/searchsoftwarequality/definition/application-security

Lumy, G. D. (2010). *Ilusi Test Penetrasi Bagian 1*. InfoKomputer.

Mardiana, Y., & Sahputra, J. (2017). *Analisa Performansi Protokol TCP, UDP dan SCTP Pada Lalu Lintas Multimedia*. *13*(2).

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2018). Analisis Keamanan Informasi Data Center Menggunakan Cobit 5. *Jurnal Teknik Informatika*, *10*(2), 119–128. https://doi.org/10.15408/jti.v10i2.7026

Maulana, M. M. (2019). AUDIT KEAMANAN SISTEM INFORMASI PADA

DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN BOGOR MENGGUNAKAN STANDAR ISO/IEC 27001:2013 DAN COBIT 5. *Jurnal Teknik Informatika*.

MCMaster University. (2022). *The Five-Layer TCP/IP Model: Description/Attaks/Defense*. MCMaster University.

Mell, P., Dugal, D., Casotto, F., Nordwall, P., & Sommerfeld, D. (2022). *NIST Internal Report NIST IR 8409 Measuring the Common Vulnerability Scoring System Base Score Equation*.

Mell, P., Scarfone, K., & Romanosky, S. (2007). The common vulnerabi-lity scoring system (CVSS) and its applicability to federal agency sys-tems, NIST IR 7435. *USA: Department of Commerce*.

Mira Orisa, & Ardita, M. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web. *Jurnal Mnemonic*, *4*(1), 16–19. https://doi.org/10.36040/mnemonic.v4i1.3213

Monteiro, A. F., Azevedo, M. V., & Sztajnberg, A. (2013). Virtualized Web server cluster selfconfiguration to optimize resource and power use. *Journal of Systems and Software*, *86*(11), 2779-2796.

Moret, W. (2014). Vulnerability Assessment Methodologies: A Review of the Literature. In *United States Agency for International Development (USAID)*.

Muhamad Mawahib, K. H. V. A. (2015). Perancangan Sistem Pelaporan Nilai Ujian Sekolah Berstandar Nasional Pendidikan Agama Islam (USBN PAI) Berbasis Web (Studi Kasus Direktorat Pendidikan Agama Islam Kementrian Agama RI). *Jurnal Teknik Informatika*, *4*(1). https://doi.org/10.15408/jti.v4i1.2014

Murni, S., & Zulham, M. (2022). PEMANFAATAN FRAMEWORK CODEIGNITER DALAM MEMBANGUN APLIKASI PENENTUAN BESARAN INSENTIF CANVASSER STUDI KASUS : PT. ARGA BOGA CEMERLANG CABANG PONTIANAK. *Jurnal Ilmu Teknik Dan Komputer*, *6*(1), 58–66.

Nur, A. (2019). Analisis dan Pengujian Kerentanan Sistem Informasi Perpustakaan. *Jurnal Mandiri*, *3*(1), 99–115.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang

Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network ( Literature Review Sim ). *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, *Vol. 3*(No. 5), 564–573.

Owasp. (2021). *OWASP Top Ten*. Owasp.Org.

Paket Internet. (2020). *Pengumpulan Informasi menggunakan theHarvester di Kali Linux*. Paket Internet. https://www.paketinternet.id/2020/09/pengumpulan-informasi-menggunakan-theharvester-di-kali-linux.html

Pandapotan, L. (2021). PENETRATION TESTING TERHADAP DAMN VULNERABLE WEB APPLICATION (DVWA) MENGGUNAKAN METODE ZERO ENTRY HACKING (ZEH) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP). *Universitas Pembangunan Nasional Veteran Jakarta*. http://repository.upnvj.ac.id/id/eprint/11657

Parmar, M. (2019). *Google Dorks*. *August*. https://doi.org/10.13140/RG.2.2.24202.62404

Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, *2008*(semnasIF), 379–386.

Perdana, R. S. (2018). AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung). *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *3*(1), 9. https://doi.org/10.32897/infotronik.2018.3.1.83

Permatasari, R. (2016). *ANALISA HASIL PENETRATION TESTING SISTEM KEAMANAN WEB DENGAN MENGGUNAKAN METODE ISSAF ( Study Kasus : UIN Jakarta )*.

Pesona, A. S. (2022). *CVSS adalah Standar Penilaian Kerentanan Sistem Keamanan*. Aplikas Servis Pesona. https://aplikas.com/blog/cvss-adalah-standar-penilaian-kerentanan-sistem-keamanan/

Prasetiadi, A. E. (2011). *Web 3.0: Teknologi Web Masa Depan*. *1*(3), 1–6.

Ratminingsih, N. M. (2010). Penelitian Eksperimental Dalam Pembelajaran Bahasa

Kedua. *Prasi*, *6*(11), 31–40.

Retna Mulya, B. W., & Tarigan, A. (2018). Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea. *ILKOM Jurnal Ilmiah*, *10*(2), 190–200. https://doi.org/10.33096/ilkom.v10i2.311.190-200

Reza, R. F. (2020). *Penerapan Keamanan Server dengan Teknik Hardening pada Sistem Operasi Ubuntu Server*. http://eprints.ums.ac.id/id/eprint/90707

Riasetiawan, M. (2016). Pusat Data untuk Pemerintahan. *Departemen Ilmu Komputer Dan Elektronik, FMIPA UGM*, 1–57. http://mardhani.staff.ugm.ac.id/files/2016/03/Pusat-Data-untuk-Pemerintahan.pdf

Run System. (2022). *Cyber Security: Pengertian, Konsep, Jenis, dan Ancaman di Bisnis*. RUN System. https://runsystem.id/id/blog/cyber-security/

Sachroni, S.H, K. I. (2020). *Patroli siber terpadu dalam penanggulangan siber crime* (Issue September). http://pustakamaya.lan.go.id/uploaded_files/temporary/DigitalCollection/ZGMyNjk3MGNkYTlmOTZhNDEyOGI4ZDhiYTNkZjQzODUxNjlhZmE0OQ==.pdf

Sahtyawan, R. (2019). Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment and Penetration Testing). *Journal of Information System Management (JOISM)*, *1*(1), 18–22. https://doi.org/10.24076/joism.2019v1i1.18

Sangga Buana, B. S., & Rijal, S. (2021). Kekerasan Terhadap Pers Melalui Serangan Siber: Studi Kasus Pada Media Online Tempo.Co. *Jurnal Studi Jurnalistik*, *3*(2), 1–20. https://doi.org/10.15408/jsj.v3i2.22983

Saputro, Y. F. D. (2014). OSI LAYER. *Ilmukomputer.Com*, 1–6. https://ilmukomputer.org/wp-content/uploads/2014/09/OSI-LAYER1.pdf

Secura. (2018). Vulnerability Assessment & Penetration Testing. In *International Journal of Recent Trends in Engineering and Research*. https://doi.org/10.23883/ijrter.2018.4135.tru9k

Snell, N. (1997). *Menjelajah Internet dengan Windows '95*. Andi Offset.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices* (4th ed.). Prentice Hall. https://doi.org/10.1088/1742-6596/1025/1/012111

Stefinko, Y., Pizkozub, A., & Banakh, R. (2016). Manual and automated penetration testing. Benefit and drawbacks. Modern tendency. In *International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)* (pp. 488–491). Lviv. https://doi.org/10.1109/TCSET.2016.7452095

Sulistyowati S.Kom., M.MT., I. (2021). *Pengantar Keamanan Sistem Komputer & Jaringan Komputer*. 1–46.

Sutabri, T. (2012). *Konsep Sistem Informasi* (I. Nastiti (ed.); 1st ed.). Penerbit Andi. https://books.google.co.id/books?hl=en&lr=&id=uI5eDwAAQBAJ&oi=fnd&pg=PA1&dq=konsep+dasar+sistem&ots=EarlPd3CyM&sig=7byiEXaSOTMcrDxcyn6-7KDxO-U&redir_esc=y#v=onepage&q=konsep dasar sistemsistem&f=false

Suyuti Ma'sum, M., Azhar Irwansyah, M., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 56–60.

Tampubolon, R. J., Poningsih, P., Solikhun, S., Gunawan, I., & Nasution, Z. M. (2021). Implementasi Filtering Firewall Dan Hardening Web Server Untuk Mencegah Serangan Http Dos Pada Dinas Lingkungan Hidup Pematangsiantar. *Device*, *11*(2), 21–29. https://doi.org/10.32699/device.v11i2.2091

Thabroni, G. (2022). *Metode Penelitian Eksperimen: Pengertian, Langkah & Jenis*. Serupa.Id. https://serupa.id/metode-penelitian-eksperimen/

The Cyber Security Man. (2018). *Understanding and Identifying Logical Ports*. The Cyber Security Man. https://thecybersecurityman.com/2018/01/05/understanding-and-identifying-logical-ports/

Ubuntu. (n.d.). *Dasar-dasar Linux*. Ubuntu. Retrieved March 30, 2023, from https://help.ubuntu.com/kubuntu/desktopguide/id/terminals.html

Ula, M. (2019). Evaluasi Kinerja Software Web Penetration Testing. *TECHSI* -

*Jurnal Teknik Informatika*, *11*(3), 336. https://doi.org/10.29103/techsi.v11i3.1996

Victor Amrizal, M.Kom, F. F. M. S. ,. (2015). Analisa Dan Komparasi Pc Router Ubuntu Dengan Router Komersil (Belkin) Di Jaringan Lan. *Jurnal Teknik Informatika*, *5*(1), 1–8. https://doi.org/10.15408/jti.v5i1.2026

Wardaya, M. S. S. (2019). *PENETRATION TESTING TERHADAP WEBSITE ASOSIASI PEKERJA PROFESSIONAL INFORMASI SEKOLAH INDONESIA (APISI)*.

Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking*. William Pollock. https://www.ptonline.com/articles/how-to-get-better-mfi-results

Who.is. (2022). *Welcome to Who.is*. https://who.is/faq

Widodo, C., Yana, M., & Agung, H. (2018). Implementasi Topologi Hybrid Untuk Pengoptimalan Aplikasi Edms Pada Project Office Pt Phe Onwj. *Jurnal Teknik Informatika*, *11*(1), 19–30. https://doi.org/10.15408/jti.v11i1.6472

Wisanggeni. (2021). *OWASP (Open Web Application Security Project) Zap*. Edy Susanto. https://edysusanto.com/owasp-open-web-application-security-project-zap/

Yudianto, M. J. N. (2014). Jaringan Komputer dan Pengertiannya. *Ilmukomputer.Com*, *Vol.1*, 1–10.

Yulianeu, A., & Wahab, A. (2017). Simulasi alat bantu pembelajaran topologi jaringan secara visual. *Jurnal Teknik Informatika*.

Yunus, M., & M. As'Ad. (2012). Protokol Tcp/Ip Sebagai Sarana Dalam Proses Transfer Data. *Jurnal Teknologi Informasi*, *3*(1), 75–93.

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1), 105–122.

# LAMPIRAN

**Lampiran 1** Surat Pernyataan Perjanjian Kerahasiaan Penetration Test

*Penetration Test Non-Disclosure Agreement*

**SURAT PERNYATAAN**
**PERJANJIAN KERAHASIAAN**
***(NON DISCLOSURE AGREEMENT)***
***PENETRATION TEST***

1. Kami yang bertandatangan di bawah ini :
   a. Nama : SRU WAHYUDI, SE
      NIP : 196611172007011003
      Pangkat/Jabatan : Penata (III/c)
      Instansi : Dinas Penanaman Modal dan Pelayanan Terpadu
      Selanjutnya disebut **PIHAK PERTAMA**
   b. Nama : Muhammad Yaqi
      NIM : 11180910000125
      Instansi : UIN Syarif Hidayatullah Jakarta
      Selanjutnya disebut **PIHAK KEDUA**

   **PIHAK PERTAMA** dan **PIHAK KEDUA** secara bersama-sama selanjutnya disebut sebagai **PARA PIHAK.**

2. Dalam rangka *Penetration Test* yang dilaksanakan oleh PIHAK KEDUA atas permohonan dari Surat dari UIN Syarih Hidayatullah Jakarta Fakultas Sains dan Teknologi Nomor B – 2234/F9/KM. 01/06/2022 Tanggal 4 Juni 2022 tentang Permohonan Riset. Dengan ini menyatakan bahwa PIHAK KEDUA diizinkan melaksanakan kegiatan *Penetration Test* terhadap aplikasi milik PIHAK PERTAMA dengan ruang lingkup:

| No | Nama Aplikasi | Alamat Situs | IP Address |
|---|---|---|---|
| 1. | Website Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan | https://dpmptsp.tangerangselatankota.go.id/ | 103.146.182.218 |

3. Pihak KEDUA hanya melaksanakan *Penetration Test* terhadap ruang lingkup tersebut di atas sesuai dengan alamat IP di atas.

**Lampiran 2** Surat Pernyataan Perjanjian Kerahasiaan Penetration Test

4. PIHAK KEDUA tidak melakukan pengambilan hak akses atau seluruh bentuk tindakan yang dapat menyebabkan perubahan konfigurasi dan mempengaruhi kinerja sistem informasi yang telah bekerja tanpa seizin dari PIHAK PERTAMA.
5. PIHAK KEDUA wajib memberikan hasil laporan dan rekomendasi terkait pelaksanaan kegiatan *Penetration Test* sesuai dengan jadwal yang telah ditentukan.
6. PIHAK PERTAMA menyediakan akses ke sistem informasi dan sarana pendukung lainnya untuk PIHAK KEDUA terkait proses pelaksanaan kegiatan *Penetration Test*.
7. Surat pernyataan ini bersifat mengikat antara PARA PIHAK. Apabila terdapat perubahan yang tidak tercantum pada klausul pernyataan ini, dapat disesuaikan berdasarkan kesepakatan bersama yang akan dicantumkan dalam laporan hasil pelaksanaan kegiatan *Penetration Test*.
8. Surat pernyataan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Jakarta, 29 September 2022

| PIHAK KEDUA | PIHAK PERTAMA |
|---|---|
| Muhammad Yaqi | SRU WAHYUDI, SE |
| NIM.11180910000125 | NIP. 196611172007011003 |

RAHASIA

**Lampiran 3** Surat Persetujuan Penelitian

PEMERINTAH KOTA TANGERANG SELATAN

**DINAS PENANAMAN MODAL DAN PELAYANAN TERPADU SATU PINTU**

Alamat : Jalan Raya Serpong, Km.16 Cilenggang, Serpong - Kota Tangerang Selatan
Email : dpmptsp.tangerangselatankota@gmail.com; Website : https://simponie.tangerangselatankota.go.id
Telepon : (021) 55698116, 55698825, 55698978, 53150117, 53150120

Tangerang Selatan, 12 Mei 2023

Kepada
Yth. Dr. La Ode Sumarlin, M. Si
Wakil Bidang Akademik
Universitas Islam Negri (UIN)
Fakultas Sains Dan Teknologi
Di - Tempat

Nomor : 500.15.6/790-Sekretariat
Lampiran :
Perihal : Persetujuan Penelitian

Menindaklanjuti surat saudara, Nomor :B-41/F9/KM.01.2/05/2023, Tanggal 12 Mei 2023, Perihal : Permohonan Persetujuan Penelitian.

Pada prinsipnya kami tidak keberatan dan menerima Mahasiswi terlampir,

| NO | NAMA MAHASISWI | NIM | PROGRAM STUDI |
|---|---|---|---|
| 1. | MUHAMMAD YAQI | 1118091000125 | S-1 Teknik Informatika/X |

Untuk melaksanakan penelitian di kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Tangerang Selatan,.

Demikian surat persetujuan ini kami buat untuk dapat dipergunakan sebagaimana mestinya.

An.Kepala
Kepala Sub Bagian Umum

**HELMI KAMALUDIN, S. Sos**
NIP. 19690720 199701 1 002

**Lampiran 4** Surat Permohonan Penelitian

**KEMENTERIAN AGAMA**
**UIN SYARIF HIDAYATULLAH JAKARTA**
**FAKULTAS SAINS DAN TEKNOLOGI**

Jl. Ir. H. Juanda No. 95 Ciputat 15412 Indonesia
Telp. (62-21) 7493606, 7493547 Fax. (62-21) 7493315

Website : fst.uinjkt.ac.id
Email : fst@uinjkt.ac.id

Nomor : B - 2234/F9 / KM. 01 /06/2022 Jakarta, 04 Juni 2022
Lampiran : -
Hal : Permohonan Riset

Kepada Yth.
Penanggung Jawab Website atau Tim Teknisi IT Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan
DINAS PENANAMAN MODAL
Di
Tempat

*Assalamualaikum, Wr Wb*

Dengan hormat kami sampaikan bahwa:

| | |
|---|---|
| Nama | : MUHAMMAD YAQI |
| Tempat/Tanggal Lahir | : TANGERANG / 10 Agustus 1999 |
| NIM | : 11180910000125 |
| Semester | : 8 |
| Program Studi | : Teknik Informatika |
| Alamat | : JL BENDA TIMUR 12 E59/23 PAMU |
| Telp/HP | : 081283472717 |

adalah benar yang bersangkutan mahasiswa Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta dan bermaksud melakukan penelitian/riset di instansi yang Bapak/Ibu pimpin, yang sedang dalam penyelesaian skripsi dengan judul skripsi:

**"MPLEMENTASI VULNERABILITY ASSESMENT DAN PENETRATION TESTING (VAPT) DENGAN MENGGUNAKAN METODE ZERO ENTRY HACKING (ZEH) TERHADAP WEBSITE DINAS PENANAMAN MODAL & PTSP KOTA TANGERANG SELATAN"**

Untuk itu, kami mohon kesediaannya untuk memberikan kesempatan kepada mahasiswa tersebut dalam melaksanakan penelitian Data/riset di instansi/perusahaan yang Bapak/Ibu pimpin.

Demikian, atas perhatian dan kerjasamanya kami ucapkan terima kasih.

*Wassalamu'alaikum, Wr Wb*

Jakarta, 04 Juni 2022
**a.n Dekan**
**Wakil Dekan Bid. Akademik**

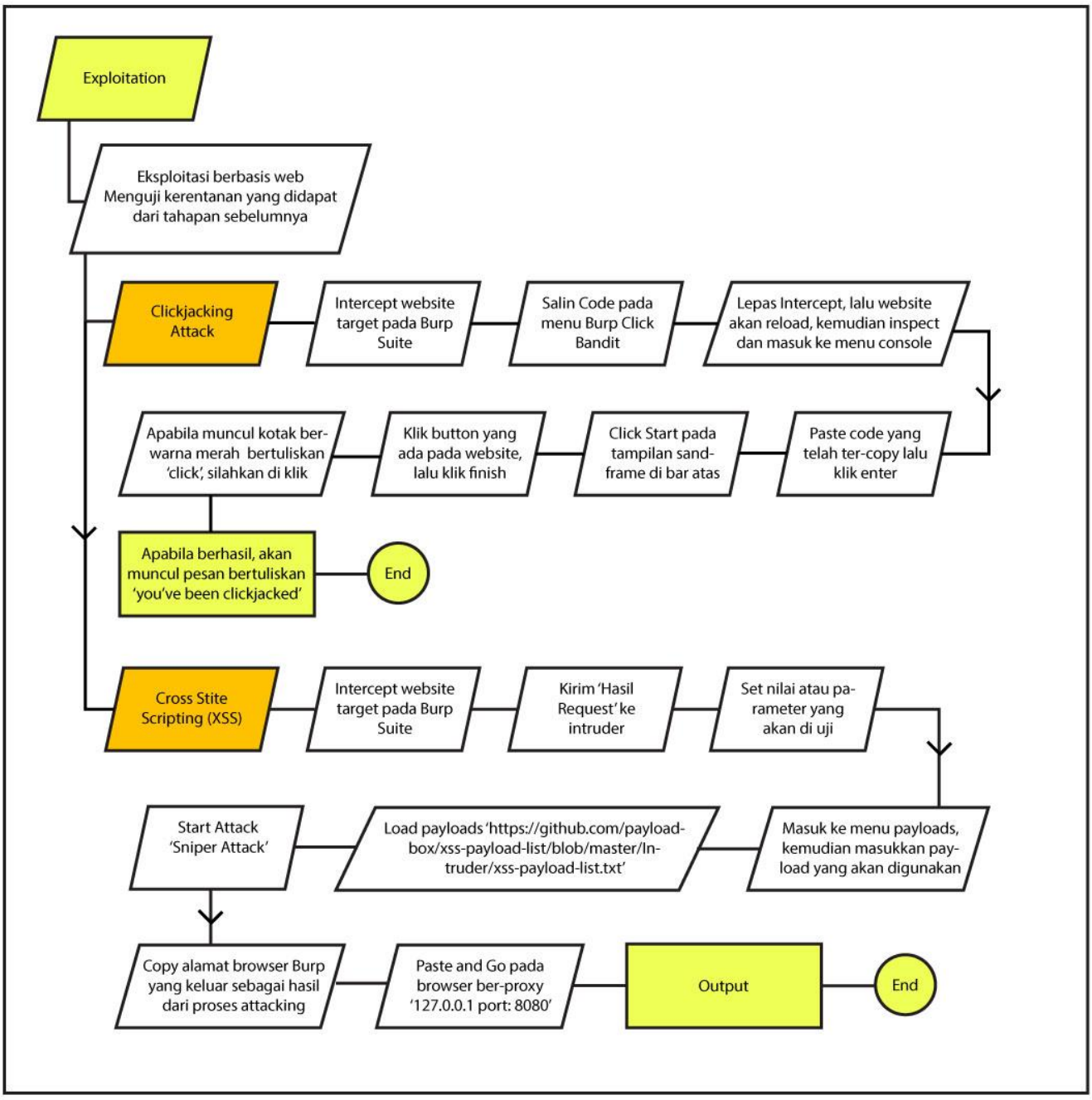
**Dr. Ir. Siti Rochaeni, M.Si.**
NIP. 196203081989032001

Cek Keaslian Surat di https://e-letter.fst.uinjkt.ac.id/scan

**Lampiran 5** Hasil Wawancara dengan Bpk. Ardan

| | |
|---|---|
| Peneliti | Apakah nama alamat lengkap website Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan? |
| Ardan | dpmptsp.tangerangselatankota.go.id/ |
| Peneliti | Siapa penanggung jawab dari website Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan? |
| Ardan | Bpk. Herly Efendy, dan Saya sendiri sebagai *staff* umum |
| Peneliti | Apakah website Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan pernah mengalami serangan siber? |
| Ardan | Belum pernah |
| Peneliti | Sejauh ini bagaimana keamanan dari web server dari pihak Dinas Investasi & PTSP Kota Tangsel pak? |
| Ardan | Untuk keamanannya , dari sisi server sudah dipasangkan honeypot dari bssn dan WAF (Web application Firwall) |
| Peneliti | Apakah Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan bersedia untuk diuji keamanan nya? |
| Ardan | Bisa diuji pantest, bisa diajukan surat pemberitahuan ke diskominfo untuk seksi persandian terkait pengujian keamanannya. |

**Lampiran 6** Hasil Wawancara dengan Bpk. Hafiz Diskominfo Tangerang Selatan

| | |
|---|---|
| Peneliti | Versi Web Sever Nginx yang digunakan itu versi berapa yaa pak? |
| Hafiz | Sudah *Up to date* menggunakan yang terbaru |
| Peneliti | Jaringan yang digunakan Dinas Penanaman Modal itu LAN, WAN, atau MAN? |
| Hafiz | Untuk lokal di data center LAN, yang akan terhubung dengan IP *Public* |
| Peneliti | Pada gambar topologi jaringan, untuk Honeypot dan WAF yang terpasang disistem keamanan itu dibagian yang mana yaa pak? (Pada Gambar Topologi Jaringan) |
| Hafiz | Honeypot ada atas *router server*, WAF agent ada di masing-masing *server client* |

**Lampiran 7** Flowchart Tahap Exploitation